Info, Comm & Ethics in Society (2004) 2: 97–109

Ethical Aspects of Facial Recognition Systems in Public Places

Philip Brey

Department of Philosophy, University of Twente, The Netherlands
Email: p.a.e.brey@utwente.nl

ABSTRACT

This essay examines ethical aspects of the use of facial recognition technology for surveillance purposes in public and semipublic areas, focusing particularly on the balance between security and privacy and civil liberties. As a case study, the FaceIt facial recognition engine of Identix Corporation will be analyzed, as well as its use in "Smart" video surveillance (CCTV) systems in city centers and airports. The ethical analysis will be based on a careful analysis of current facial recognition technology, of its use in Smart CCTV systems, and of the arguments used by proponents and opponents of such systems. It will be argued that Smart CCTV, which integrates video surveillance technology and biometric technology, faces ethical problems of error, function creep and privacy. In a concluding section on policy, it will be discussed whether such problems outweigh the security value of Smart CCTV in public places..

1. INTRODUCTION

After the American Super Bowl XXXV in Tampa, Florida in June 2001, a major controversy ensued. It became public that police had used video cameras equipped with facial recognition technology ("facecams") to scan the faces of the 100,000 visitors to the Bowl in search of wanted criminals. Many people were outraged, and this Super Bowl has since been dubbed the "Snooper Bowl" (Lyman, 2001) Although not well known to the general public, facial recognition technology is nowadays used in many places across the world. It is used for a variety of purposes, one of them being surveillance in public areas, as in the Super Bowl. Even at the time Super Bowl XXXV, facecams were already in use in several cities, including cities in the U.S. and the U.K, for routine surveillance of public areas.

Since the September 11 terrorist attacks, just months after the Super Bowl event, federal governments and airports have taken an interest in the technology as an instrument in the fight against international terrorism. It is currently in trial use in several international airports in Europe and the U.S., including Keflavik Airport in Iceland, Boston's Logan Airport, Dallas-Fort Worth International and Palm Beach International Airports (Kopel and Krause, 2002). Moreover, the American Enhanced Visa Entry Reform Act of 2002 will require all Americans and all non-U.S. citizens visiting the U.S. to have a passport with a biometric chip that contains their encoded facial features by October 2004. This data would then be checked with a database of suspected criminals and terrorists upon arrival in the U.S. This measure follows the recommendations of the International Civil Aviation Organization (ICAO),

KEYWORDS

Facial Recognition Systems

Ethics

which earlier ruled that facial recognition technology should be the the method used to identify travelers worldwide and who is proposing a global database that encodes passport information and facial features of all passport holders worldwide (Bergstein, 2003). The European Union is also working on new passports with facial biometrics.

In this paper, I will examine ethical aspects of the use of facial recognition technology for surveillance purposes, focusing particularly on the balance between security and privacy and other civil liberties. My ethical analysis will be based on a careful analysis of current facial recognition technology, of its use in video surveillance (CCTV) systems, and of the arguments of proponents and opponents of such "smart" CCTV systems. From an ethical point of view, Smart CCTV is interesting because it involves two contested technologies: video surveillance technology and biometrics. I will examine how ethical objections to Smart CCTV (or facecams) refer to objections to these two broader types of technology.

To focus my discussion, I will be discussing a particular facial recognition technology, the FaceIt engine that has been developed by Identix, a leading developer of identification technologies and systems. In the next section, I will carefully analyze the technology behind the FaceIt engine and consider the types of applications for which the engine is used. In section 3, I will consider the use of the FaceIt engine in Smart CCTV systems in public places, focusing specifically on their use in the Ybor City district of Tampa, Florida. I will describe the particular system that is used, as well its users, the setting in which it is used, and the purposes for which it is used. In section 4, I will turn to the debate on Smart CCTV, focusing again on Ybor City as a case. I will outline the arguments used by proponents and opponents of the system, and identify the values and assumptions that underly these arguments. This will then lead me to a straight-on discussion of the ethical aspects of facecams in section 5, where I will critically discuss three problems with the use of facecams: problems or error, function creep and privacy. In section 6, I conclude with a policy discussion of the use of facecams in public places.

2. FACIAL RECOGNITION TECHNOLOGY: THE FaceIt ENGINE AND ITS APPLICATIONS

There are now several firms that market facial recognition technology. Some of these specialize in the development of facial recognition software, whereas others specialize in the implementation of complete systems consisting of both hardware and software. The core of a facial recognition system, however, is its software, and specifically the software that is capable of analyzing digital images and recognizing faces in them. I will here consider one such program, or 'software engine,' the FaceIt® software engine of Identix Corporation. The FaceIt engine is the currently most widely used facial recognition technology and is and also one of the most advanced systems on the market. The FaceIt engine was originally developed by Visionics Corporation, which merged in 2002 to become Identix. Identix is a U.S. corporation based in Minnetonka, Minnesota, with over 500 employees worldwide, and is the current worldwide leader in identification technologies and systems, including fingerprint identification and facial recognition technology.[1]

FaceIt is a software engine that is run on a computer to detect and recognize human faces. It takes as its input digitally encoded images, which are either digitally coded photographs or still images obtained from streaming video, and "scans" them for faces. The engine can be used for mere *face finding*, which is locating one or more faces in an image. However, its more customary use is that of *face recognition*: comparing a face found in an image against a database of facial images in order to find a match. Such face recognition can be organized in two ways. In *one to one matching*, also called verification or authentication, the system is used to determine if a face matches an entry in the database. In *one to many searching*, or *identification*, a list of matches is generated for those entries in the database that are above a certain threshold similarity to the input face. Next to face finding and face recognition, the engine is also capable of *tracking*: following the face of a person in a video field of view as the person moves around.

The FaceIt engine works by analyzing up to eighty facial points around the nose, cheekbones and eyes in a facial image. It can do this by means of a specially developed mathematical technique called Local Feature Analysis (LFA). This technique is based on the assumption that a facial image is built up out of a finite number of facial building elements, or features, that vary in each face and that may moreover have different positions relative to one another. Such building elements and their relative positions are detected using a complex algorithm, and are then encoded into a complex mathematical formula called a *faceprint*. A faceprint is a mathematical formula that is unique to a person's face. It is moreover resistant to changes in lighting, skin tone, eyeglasses, hairstyle and facial hair, and is also indifferent to the angle at which a face is observed, as long as the eyes are clearly visible. Faceprints come in two sizes: a light version of just 88 bytes and a detailed version of 3.5 Kilobytes.

Faceprints have several advantages over mere digitized facial images for the purpose of facial recognition. First, they specify features that are unique to an individual's face and distinguish it from millions of others, without including information that may be different in different circumstances, such as lighting, facial angle, facial expression and eyeglasses. Second, they can be processed at much greater speed than facial images. Using a 733 MHz Pentium III CPU, for example, a FaceIt engine can search up to 1 million faceprints per second. Third, they allow for very precise and reliable estimates of the degree to which two facial images match each other. According to Identix, the error rate for matches of facial images of good quality is less that one percent.

The FaceIt engine is a software engine, not a complete hardware system. It can be combined with various types of hardware and software to create different kinds of face recognition systems. Moreover, the engine itself can be configured in different ways, to accommodate for specific contexts and purposes of use. This means that the FaceIt engine is extremely flexible, and allows for a very broad range of applications. Currently, the engine is used in four broad types of applications: authentication systems, identification systems, criminal justice database systems, and surveillance systems.

When used as an *authentication system*, the FaceIt engine is used to secure transactions and to clearly associate each action with the identity of the person who is conducting it. In this modality, it may serve as a replacement of a password or PIN, and may be used for access control, border control, computer and network security, and banking transactions. Currently, FaceIt is used in all these capacities, ranging from its use as a biometric screensaver in SONY laptops to its use in a border crossing system by the Israeli Ministry of Defense to manage the flow of individuals entering and exiting the Gaza Strip.

When used as an *identification system*, the engine is used to compare the picture on ID documents (such as passports, driver's licenses, etc.) with a database in order to detect identity fraud, which may occur in the form of identity theft, duplicate aliases, and fictitious identities. The engine has been used, for example, in the July 2000 election in Mexico to search for possible duplicates in voter registration records, and is also used in many driver licensing and social service benefits systems. Used in *criminal justice database systems*, the engine allows law enforcement agencies to compare photographs (usually, mug shots) of suspects with the images in its databases. In 2001, the engine was used in this capacity by law enforcement agencies in eight U.S. states.

The use of the engine as a *surveillance system* is the use that I will be concerned with in the remainder of this paper. In this type of application, the engine is used to recognize faces at a distance, often in a crowd or in an otherwise complex scene, or to follow the presence or position of persons in a video field of view. Such surveillance is performed with the use of one or more video cameras. Often, the system is a stationary CCTV system, which is then sometimes called "Smart CCTV"; the cameras that are used are sometimes referred to as "facecams." Surveillance using face recognition technology can have various purposes, such as identifying criminals or terrorists, identifying missing persons, identifying VIP guests or customers, and tracking suspicious characters. In this capacity, the FaceIt engine is currently used in town centers, airports, casinos, construction job sites, and various other places.[2]

3. USING FACECAMS: VIDEO SURVEILLANCE IN PUBLIC PLACES WITH 'SMART CCTV'

In discussing 'smart' video surveillance, I will focus on its use in public city areas. I will not discuss its use in the private sector, in which it is not used very often anyway (e.g. it is used as a time and attendance system by a British civil construction firm) (Visionics, 2001). I will also pay little attention to places that are privately run but nevertheless publicly accessible (e.g. airports,[3] casinos and stores[4]); I will only briefly consider its use in airports.

Smart CCTV is only used in a small number of public city areas worldwide. In 2001, the FaceIt engine was used in three public city areas worldwide, one in the U.S. and two in the United Kingdom. Only a few have followed since. The first city to adopt the FaceIt system for surveillance purposes was London, who started using it in October 1998 in the neighborhood of Newham. In 2001, the system was tied to 300 CCTV cameras in this neighborhood, which are linked to a central CCTV control room operated by London Metropolitan Police Service. In April 2001, the FaceIt system was deployed in Birmingham, U.K., where it was integrated in the CCTV system already in place in the city centre. In June 2001, Tampa, Florida became the first American city to start using Smart CCTV. The Tampa police department started using FaceIt in its CCTV system that was already in place in the Ybor City entertainment district.[5]

Smart CCTV is only used in a small number of public city areas worldwide

In all three cities, the system is used in a busy neighborhood, and involves a CCTV system with a large number of video cameras. In all three cities, also, the system is operated by the city police department, and is used for routine surveillance, meaning that people in the area will be routinely scanned and have their faces searched in a database. In all three cities, also, the main purpose of the system is to identify known criminals or criminal suspects with an arrest warrant, so that they can be monitored or stopped and arrested. In 2002, the police department of the American city Virginia Beach started using a Smart CCTV system with the FaceIt engine at the beachfront, thus becoming the second U.S. city to use a Smart CCTV system. This system gained a somewhat broader use: not only to identify criminals, but also to help locate lost children and missing persons.[6]

My focus in the rest of this paper will be on the Tampa system, and the controversy it has sparked. The system used in Tampa came into operation on June 29, 2001, and was added to an existing CCTV system that had already been in use since 1998. The system, run by the Tampa police department, included 36 cameras in the historic Ybor City entertainment district, a popular district in the centre of Tampa that is frequented by tens of thousands of locals and tourists every day. The cameras, that have the ability to tilt and pan, were linked to a central command post that includes ten video screens and computers running the FaceIt software. The cameras were concentrated in the Centro Ybor entertainment complex and along E Seventh Avenue. Pedestrians were informed about the cameras by curbside warning signs reading "Area under video monitoring" and "Smart CCTV is in use".

The system was linked to a database consisting of known felons on active warrants (the most important category), people convicted of past sexual offenses in the state of Florida, and missing children and runaway teens. In 2001, the database consisted of 30,000 images of individuals in these categories, with plans to further enlarge the database.[7] The system engages in constant, automated monitoring of pedestrians. If there is a resemblance during a matching process, the computer will rate it from 1 to 10, sounding an alarm for matches of 8.5 and above. The officer doing the monitoring will then alert others on the street by radio, who will stop the person and determine their identity. If they are wanted, they will be arrested. If they are not, the situation will be explained to them, and they are free to go.

The police department became interested in the software after it had been approached by Visionics Corp., the devel-

oper of the software, which later merged to become Identix. Use of the software required approval of the city council, which was granted in May 2001, a month before the system was put in use, in a meeting that did not include a public hearing. Since then, some public protests have ensued and some council members voiced concern about the technology and claimed they did not realize what they had voted for in their earlier vote. A second vote was held on June 19, after a public hearing, that resulted in a 3-3 split vote in the council, with the mayor casting the deciding vote. He voted to give the Tampa police permission to install the system, which was subsequently installed on June 29. A motion was brought to the floor in August 2001 by two council members to terminate the contract with Visionics Corp. The motion was rejected on a 4-2 vote.

4. THE DEBATE ON FACIAL RECOGNITION TECHNOLOGY: PRIVACY VERSUS SECURITY

The Tampa Smart CCTV system has generated a lot of debate, as has Smart CCTV and facial recognition technology in general. In this section, I will identify participants in the debate on Smart CCTV, with special emphasis on Tampa-based participants, and consider the main arguments used by both proponents and opponents of the technology. All references are to 2001, which is the year in which the system was installed. I will show that, perhaps predictably, the debate on Smart CCTV was strongly centered around the notions of privacy and security, with proponents arguing for the security benefits of the technology, and opponents emphasizing its threat to privacy. I will also attempt to show that certain types of arguments are repeated over and over in this debate.

In the Tampa debate on facecams, nearly all vocal participants are either proponents or opponents of the technology. The proponents include, of course, the manufacterers, i.e. Identix' predecessor Visionics Corp. along with its industrial partners. They also include members of the Tampa police department which has adopted the technology, supportive local government officials and citizens who support the technology. Opponents include city council members and citizens who oppose the technology, as well as privacy and human rights groups and media critics who have chosen to participate in the debate. The privacy and human rights groups that have been involved with the Tampa case include the Tampa Electronic Privacy Information Center (EPIC) and the American Civil Liberties Union of Florida.[8] Also involved has been the Law Enforcement Alliance of America (LEAA). The backdrop of the Tampa debate is a wider media debate on facial recognition technology that was picking up steam in 2001.

The security vs. privacy dimension is very visible in the Tampa debate, as well as in the wider media debate. Proponents typically argue that the technology has significant security benefits and minimal privacy losses, and that any privacy losses are in any case offset by the great security benefits. Opponents typically argue that the security benefits are overestimated and the privacy losses are underestimated by the proponents, and that the costs to privacy of the technology are greater than the gains in security. Importantly, not all arguments used by opponents refer to privacy as an eroded right; some refer instead to the erosion of individual freedom. Some, for example, claim that an arrest of an innocent citizen based on an incorrect match is a violation of personal freedom, and not of privacy.

Let us first consider statements in the debate that address the *security value* of the technology. Proponents argue that the technology is highly valuable as a means to reducing crime and enhancing security and the quality of life in neighborhoods, because it is an effective and accurate technology. Detective Bill Todd of the Tampa police department, who is in charge of the operation in Ybor City, has called the technology a "powerful tool to assist in maximizing public safety".[9] City councilman Robert Buckhorn calls it a "public safety tool" (Canedy, 2001). The belief in safety is echoed by citizens in favor of the system, like Gil Rizzo, a 42-year old account representative in Tampa, who claims "I'm in favor of it because of the security. A lot of nights, there has been shoplifting, women got mugged and robbed. It's safer because

of the cameras" (Canedy, 2001).

Indeed, proponents make frequent reference to the alleged value the technology has in stopping crime, and arresting criminals like murderers, drug traffickers and sexual offenders. They also refer to the added feeling of security that the technology may bring. For instance, John Woodward, author of a 2001 RAND report in favor of facial recognition technology, writes: "Many parents would most likely feel safer knowing their children's elementary school had a facial recognition system to ensure that convicted child molesters were not granted access to school grounds" (Woodward, 2001). Several proponents also point out another societal value of the technology, which is the location of missing persons and runaways. Opponents do not usually deny the importance of stopping crime and locating missing persons, but often question if the technology is sufficiently reliable and effective as a means for stopping crime - or simply deny that it is. For example, Kate Rears of EPIC has pointed out that the technology is not proven and that similar technology did not help to make any arrests when used in the XXXVth Super Bowl.[10]

Let us now turn to statements that address implications of the technology for privacy and freedom. Opponents of the technology emphasize that it poses a real threat to privacy and freedom. Randall Marshall, of the American Civil Liberties Union of Florida, emphasized the "Big Brother feel" of the technology, and claimed that using the technology amounts to subjecting the public to a digital lineup. ACLU Associate Director Gregory Nojeim made the same comparison, claiming: "If this isn't Big Brother, I don't know what is."[11] Jason Skinner, a security guard in Ybor, said "It's invading people's privacy. They're all over the place" (Canedy, 2001). Ryan Rovelto, a clerk in Ybor City, said "It's kind of like a police state. Whether I have a warrant or not, it makes me uncomfortable they can pick me out of a crowd and run my image" (Herdy, 2001). There have also been public protests to the technology used in Ybor City in which privacy was the issue. Just before the introduction of the technology, a hundred people protested in Ybor City, wearing signs like "We're under house arrest in the land of the free" and shouting slogans like "Big Bro, hell no" (Kasindorf, 2001). Some opponents also questioned the accuracy of the system and voiced their fear that the system would result in matches that wrongly identified innocent citizens as criminals, thus violating their civil liberties.

A different form of opposition has come from the Law Enforcement Alliance of America (LEAA), a coalition of law enforcement professionals, crime victims and concerned citizens with over 65,000 members. The LEAA issued a statement on 3 July 2001 calling for the immediate removal of the Tampa system because it represents a violation of people's 4th amendment right to privacy. The argument of the LEAA was not, however, that surveillance with Smart CCTV is not compatible with privacy rights. Rather, their argument was that system in Tampa violates the privacy policies that the manufacturer, Visionics, had subscribed to as a member of the International Biometric Industry Association (IBIA). As the LEAA pointed out, he IBIA policy claims that "clear legal standards should be developed to carefully define and limit the conditions under which agencies of national security and law enforcement may acquire, access, store and use biometric data." The LEAA claimed that since no such legal standards were in place, the system was in violation of the manufacturer's privacy policy and should therefore be removed.[11]

Proponents of the system addressed the privacy issue in various ways. Some simply denied that there is a privacy issue. City Councilman Robert Buckhorn claimed that in the public streets of a crowded neighborhood like Ybor City, "your expectation of privacy is somewhat diminished, anyway" (Canedy, 2001). This sentiment was echoed by law professor Erwin Chemerinsky of the University of Southern California, who claimed in relation to face recognition technology: "We have no reasonable expectation of privacy in a public place – that we're not going to be seen, or that our picture won't be taken" (Kasindorf, 2001). Detective Bill Todd of the Tampa police called the privacy issue overblown because he claimed that the cameras do not record images of people when they are not recognized to match an image in the database; when there is no match, people's facial images are immediately discarded. Some citizens also felt that

the privacy issue is overblown, because they did not find the technology to be invading their privacy. Said Jill Wax, owner of a clothing store in Ybor: "I don't find it an invasion of my privacy, and my customers don't either" (Canedy, 2001). Some proponents made the argument that the technology merely automates a procedure that has not previously been seen to violate privacy. City Coucilman Robert Buckhorn claimed that the technology is "no different than having a cop walk around with a mug shot" (Canedy, 2001); this is, incidentally, the exact same argument that had been made by Police Chief A.M. Jacocks of Virginia Beach, who had lobbied to get the technology accepted in that city.[12]

Next to those proponents of the technology who either deny or downplay the threat to privacy, there are others who do recognize it as a potential problem. Visionics, for one, acknowledged, along with RAND, that Smart CCTV can lead to violations of privacy. However, Visionics and RAND both claimed that such violations can be minimized when the proper safeguards are put into place. Visionics, now Identix, has argued, along with others in the biometrics industry, for legislation regulating the use of facial recognition technology, and has proposed a set of "industry-established" privacy guidelines, that include the rules that "Clear signage has been posted throughout the area indicating that "Smart CCTV" is in use; The images in the database are those of known offenders; Non-matching images are discarded from the system once the comparison has been conducted" (Visionics, 2001b).

Proponents who recognized that facecams can negatively affect personal privacy still favored the system because they believed that in the trade-off between privacy and security, the security gains are much greater than the losses in privacy and liberty. Both Visionics and Tampa police claimed, for example, that the chance of a false arrest is acceptable trade-off for the possibility of arresting a criminal who might otherwise remain at large. And Woodward claimed in his RAND report: "We should not let the fear of potential but inchoate threats to privacy, such as super surveillance, deter us from using facial recognition where it can produce positive benefits" (Woodward, 2001).

Opponents make different trade-offs. Philip Hudok, a concerned citizen commenting on plans to install Smart CCTV in Virginia Beach, stated: "I wouldn't even go near the vicinity of a place that condones this. There's no benefit great enough to sacrifice this much personal privacy."[14] Thomas Greene, an author commenting on the RAND report in favor of facecams, complained that the author of the report "reckons that the natural rights of the majority of ordinary, law-abiding citizens should be sacrificed for the sacred mission of identifying and prosecuting a mere handful of sexually perverted or homicidal lunatics." He went on to claim: "Surely, the suffocating, risk-free environments our governments are trying so desperately to sell us to extend their powers of observation and control are far more grotesque and soul-destroying than anything a terrorist or a pedophile might ever hope to produce" (Greene, 2001).

Next to those proponents of the technology who either deny or downplay the threat to privacy, there are others who do recognize it as a potential problem

5. ETHICAL CONSIDERATIONS FOR THE USE OF FACECAMS

The privacy versus security debate on Smart CCTV is about a genuine issue, since security and privacy may easily come to stand in opposition to each other. And just like opponents of facecams cannot easily discard their potential security benefits, proponents cannot easily sidestep the threats they pose to civil liberties. Trade-offs will therefore have to be made between security and civil liberties in deciding whether and how to use facecams. What is needed, most of all, is a better understanding of how trade-offs *can* be made: how much infringement of civil liberties can be justified by reference to security concerns? The debate on this question has, unfortunately, been shallow so far. What has been lacking is a good understanding of what is

at stake with facial recognition technology, and what consequences its use can bring. A better understanding is needed of both the importance of civil liberties and the importance of security, of the power and reliability of the technology, and of its potential uses and abuses. In helping to clarify some of these issues, I will now analyze three particular problems that have been associated with Smart CCTV, and address their moral implications. These are the problem of error, the problem of function creep, and the problem of privacy.

Error

The *problem of error* is mentioned repeatedly by opponents of facecams. This is the problem that with face recognition technology, incorrect matches can occur that cause innocent citizens to become subjected to harassment by police. Problems of error are not unique to facial recognition technology, but may occur with any database system that stores personal information: the database may contain erroneous personal information that may lead to cases of mistaken identity, it may be used incorrectly, with the same consequences, or its matches are based on probability estimates and therefore have a margin of error. That errors may occur was already demonstrated in the first few weeks in which the Tampa system was used: the system yielded several false positives. Moreover, a feature article in a newspaper on the systems, accompanied by still images of several scanned faces, led to an attempted arrest of one of the men in the pictures because a reader falsely believed that he was her ex-husband, who had a warrant for child neglect charges (Kopel and Krause, 2001).

However, if the problem of error is kept distinct from the problem of privacy and privacy rights, which I will discuss later, then it must be concluded that the occurrence of errors does not, in itself, present a strong case against facecams. It would only do so if the error rate is so great, and the success rate of the technology in reducing crime so low, that the apprehension of one felon would require the stopping and questioning of dozens of innocent citizens. The question is, therefore, if a good ratio can be attained between false and true positives, and if the questioning of individuals who may be false positives can be done in way that is not too obtrusive. If so, then from a purely pragmatic point of view, the trade-off may well be acceptable. After all, the public tends to accept the idea that it has to suffer minor inconveniences so that criminals can be apprehended. It accepts, for example, that it is questioned or even searched when boarding a plane, or visiting a rock concert or football match.

So the problem of error, when considered separately from the more profound problem of privacy, may not in itself present a strong argument against facecams. It does suggest, however, that there are problems with installing and using a system that is inaccurate, because it yields many false positives for each true positive. In that case, the harm done to innocent citizens that turn up as false positives may begin to outweigh the benefits of a few additional arrests of wanted criminals.

Function creep

A second, and more pressing, problem with facecams is the problem of "function creep," an expression that I borrow from RAND report author John Woodward. Function creep is the phenomenon by which a technology designed for a limited purpose may gain additional, unanticipated purposes or functions. This may occur either through institutionalized expansions of its purposes or through systematic abuse. In relation to Smart CCTV, it is the problem that, because of the flexibility of the technology, the purposes for which the system is used may be easily extended from recognizing criminals and missing persons to include other purposes.

There are, I claim, four basic ways in which Smart CCTV can become the subject of function creep. The first is by *widening of the database*. The databases used in London, Birmingham, Tampa and Virginia Beach only included felons on a warrant, past sexual offenders and missing persons. Such databases can be easily expanded with the use of already existing databases such as those of the departments of motor vehicles (DMVs) in the U.S., which include digitized photographs of licensed drivers. It is relatively easy, then to include new categories of people that are to be monitored, like people with misdemeanors, political

activists, or people with a certain ethnic background. Needless to say, some of these expansions, if they were to occur, would be morally highly problematic.

The second way in which function creep may occur is by *purpose widening*. This is the widening of the purpose for which the technology is used. For example, a police force using Smart CCTV may start using it not only to identify wanted individuals in crowds, but for example to do routine analysis of the composition of crowds in public places, or to do statistical analysis of faceprints for the purpose of predicting criminal activity, or to track individuals over longer distances. Smart CCTV has the potential to do these things, and police departments may be tempted to use the technology for such additional purposes in their efforts to fight crime and improve the quality of life in neighborhoods.

A third way for function creep to occur is by *user shifts*. Systems, once developed, may come to be used by new types of users. For instance, the FBI or CIA may require access to a system used by a police department in a search for terrorists. Or a city government or commercial organization may ask a police department to use the system for its demographic research. Also, individual operators may be using the system for their own personal reasons. As Reuters journalist Richard Meares reports, there have been several occurrences of CCTV operators being sacked because of their repeated abuse of the system, for example by tracking and zooming in on attractive women (Meares, 2001).

A fourth and final occurrence of function creep lies in *domain shifts*: changes in the type of area of situation in which the system is used, such as changes from city neighborhoods to small villages or nature parks, or from public to private areas, or from domestic areas to war zones. Function creep in Smart CCTV may hence occur in several ways, which may add up to result in new uses of the technology for new purposes by new users in new domains. Studies of technology use have shown that function creep almost invariably occurs when a new technology is used, and should therefore be taken into account (Amato, 2001; Mieszkowski, 2001). Function creep can be limited by strict regulation of the technology (which is not currently into place), but cannot be wholly avoided. This imposes an obligation on the developers and users of the technology, therefore, to anticipate on function creep and to take steps to prevent undesirable forms of function creep from occurring.

Privacy

The problems of error and function creep do not really address the problem with facial recognition technology that many of its opponents hold to be central to it: its alleged violation of personal privacy. Regardless of whether error or function creep occurs, the question is whether the very use of Smart CCTV surveillance in public places violates a basic right to privacy. Some of the proponents cited above argue that it does not, because people in public places do not have a strong expectation of privacy anyway. In an important essay, Helen Nissenbaum has argued that even if the expectation of privacy is diminished in public places, people still have justifiable privacy expectations even when they are in public (Nissenbaum, 1998). She argues that surveillance in public places that involves the electronic collection, storage and analysis of information on a large scale often amounts to a violation of personal privacy.

Nissenbaum's argument for privacy in public rests on two premises. First, citing empirical data, she claims that many people are dismayed when they learn that personal information is collected about them without their consent, even when they are in public places. This negative response shows that many people do indeed have some privacy expectations even when they are in public spaces. Second, she argues that these popular sentiments can be justified by analyzing characteristics of public data harvesting through electronic means that make it quite different from the everyday observation of people in public places. She argues that electronics harvesting involves two types of practices that raise privacy concerns. The first is the practice of *shifting information* from one context to another. The second is the combination or *aggregation* of various sources of personal information to yield new information.

The first practice described by Nissenbaum, of shifting information, is the use of electronically collected information

in a different context than the one in which it is collected. For example, information about people's supermarket purchases may be sold to a list service for magazine subscriptions, or information collected for scientific purposes may be used in a political context. Nissenbaum argues that when people divulge personal information, they tailor the amount and type of information they disclose to the context in which they disclose it. People provide doctors with details of their physical condition, discuss their children's problems with their children's teachers, and divulge financial information to loan officers at banks. She argues that there are norms – both explicit and implicit – that govern how much information and what type of information is fitting for what context.

Nissenbaum next introduces the notion of *contextual integrity*. When information-governing norms are respected, Nissenbaum claims, contextual integrity is maintained, whereas a violation of information-governing norms violates contextual integrity. Nissenbaum's point is that the practice of shifting information often violates contextual integrity: it often violates the trust that people have that information appropriate to one context will not be used in a context for which it was intended and in which it is not deemed appropriate. Yet, the practice of shifting information is very common in public data harvesting, and relatively few limitations have been imposed, by law or by custom, to prevent data collectors from using personal information in different contexts. Public data harvesting is therefore a practice that cannot be trusted to maintain contextual integrity. Nissenbaum claims that contextual integrity is one of the conditions of privacy, and that therefore, the practice of shifting information in public data harvesting poses a privacy problem.

Next to information shifting, Nissenbaum identifies aggregation as another practice in the collection and use of public data that violates privacy expectations. Aggregation is known variously as "profiling," "matching," data aggregation" and "data mining," and is the practice in which different sources of information about people are aggregated to produce databases that include complex personal records. For instance, there are bureaus that combine publicly available personal information such as drivers' license and motor vehicle records, voter registration lists, Social Security number lists, birth records and information from credit bureaus, to devise comprehensive profiles of individuals that indicate such things as their purchase power and purchasing activity. This is just one example: Many organizations in both the private and public sector engage in some form of data aggregation. Nissenbaum argues that the main objection to data aggregation is that its profiles are capable of exposing people in ways that the isolated bits of information out of which aggregates are composed are not capable of. They may reveal personal information that people could never dream would be revealed about them on the basis of isolated public bits of personal information that are much less privacy-sensitive. Hence, Nissenbaum argues, aggregation is a practice that frequently violates reasonable expectations of privacy.

Shifting information and aggregation can both be seen as instances of function creep. Shifting information corresponds, particularly, to what I have called purpose widening and user shifts, and aggregation can be seen as an instance of purpose widening. This shows that the problems of function creep and of privacy are linked: when function creep occurs, privacy is often violated as a result. However, it does *not* follow that privacy violations resulting from the use of Smart CCTV are always the result of function creep. Privacy may also be an issue when no function creep occurs. Let us suppose, for example, that very strict regulation and norms are to govern the use of Smart CCTV so that the occurrence of function creep is minimal: images of people in public places are only matched against a database of known offenders and images are discarded immediately if no match is found. Is there no privacy issue involved in this case?

Nissenbaum's analysis supports the notion that privacy may then still be an issue. This is the case because the very practice of matching faces of people in public places against faces in a database of wanted criminals appears to violate contextual integrity according to norms held by many. Many people who willingly show their face in a public place would not willingly participate in lineup at a police station, especially not if they had been picked

for the lineup because they resembled a composition sketch of a suspect. Yet, the presence of Smart CCTV in public places leaves them with no choice: they cannot choose not to divulge personal information about their facial features that will be used in a context in which they may not want it to be used. Nissenbaum argues that at the heart of our concept of privacy is the idea that privacy protects a "safe haven," a sphere where we people are free from the scrutiny of others, and within which they are able to control the terms under which they live their lives. Different people draw this sphere differently. Yet, many seem to hold that Smart CCTV takes away too much of this control, by subjecting them to routine large-scale scrutiny when they frequent public places.

Next to this privacy objection derived from Nissenbaum's analysis, another privacy objection against Smart CCTV may be made. Smart CCTV is a form of biometric technology, and this type of technology has been claimed to involve special privacy issues (Hes *et al*., 1999). The main issue is that biometric technologies digitally encode a highly personal aspect of one's body, like a thumb print, iris pattern, or face. Two things happen because of this. First, this aspect of one's body acquires a new meaning or function: it is now enrolled in a larger functional, rationalized system of identification or authentication in which it plays a specific functional role that is comparable to that of other identifiers like passwords, PIN numbers, and bar codes. In the context of this functional system, one's body part is nothing more than an information structure. For example, the unique features of one's face, by which others recognize you and which helps to define your uniqueness, can be encoded into a computer file of only 88 bytes. This functional reduction of body parts to information structures is one that many people find dehumanizing.

Second, this process of functional reduction involves the creation of informational equivalents of body parts that exist outside their owner and are used and controlled by others. There is hence not just a process of reduction occurring, but also one of alienation: the faceprint that uniquely characterizes your face is not 'yours,' but 'theirs': it is not owned by you and even if it were, it would not be understood by you because you do not understand the technology. In this way, people may come to feel that some of their body parts are no longer completely 'theirs,' because they have acquired meanings that their owner does not understand, and uses that are partially realized outside their own body.

Facecams hence pose a dual privacy problem: they face the same privacy problems that apply to surveillance cameras and public data harvesting more generally, and they also face the privacy problems that apply to biometric technologies. Moreover, a case can be made that these problems are intensified in facecams: the privacy problems with surveillance cameras are enhanced in facecams because of the additional tracking and monitoring functions afforded by such cameras, and the privacy objections raised to biometric technology can be expected to apply especially to facial recognition technology, because the human face has always been regarded as the most unique and distinguishing aspect of the human body. For these reasons, then, the debate on facecams is not likely to go away very soon.

6. POLICY ISSUES

It follows from my discussion that before Smart CCTV can be used in an ethically responsible way, three ethically charged issues first have to be dealt with in a satisfactory way. They are the problems of error, function creep and privacy. I will now briefly discuss, for each, the conditions that must be realized for them to be handled satisfactorily, the requirements this imposes on the technology and the policies that must result that regulate its use. I will also briefly assess the prospects that these conditions and their resulting requirements are indeed met.

before Smart CCTV can be used in an ethically responsible way, three ethically charged issues first have to be dealt with

To effectively deal with function creep, it seems clear that legal standards must be developed for the use of facial recognition

technology that specify which uses are authorized and which ones are not, and specify the conditions under which users may share or aggregate information. The need for such legal standards also recognized by the industry itself, as remarked in section 4. The industry's organization for this, IBIA, has developed its own good use guidelines and called for legislation to specifically address the use of biometric technologies. Identix, which is a member of IBIA, also emphasizes the importance of legislation, and has developed additional ethical policies for the proper use of its products. So function creep is currently an issue for visual recognition technology, largely because of the absence of clear legislation for its use. However, if detailed legal standards were to be adopted in the future and strictly adhered to, then the problem of function creep may become less significant.

The problem of privacy is more profound than the problem of function creep, because it is not a problem that may be "solved" through regulation or through a redesign of the technology. It could even be argued that privacy is an absolute right and that therefore the use of Smart CCTV in public areas cannot be warranted under any circumstances. Such an absolutist position would, however, automatically entail that privacy is more important than security. Yet, security entails protection from harm, which correspond with very basic rights such as the right to life, liberty and property. So it will not do if opponents of the use of Smart CCTV claim that it violates privacy and that privacy is an absolute right. It would have to be shown, rather, that its violation of privacy trumps the added security, if any, that Smart CCTV offers.

Three questions seem relevant in this privacy vs. security debate: How much added security results from the use of Smart CCTV? How invasive to privacy is the technology, as can be judged from both public response and scholarly arguments? Are there reasonable alternatives to the technology that may yield similar security results without the privacy concerns? I will not try to answer all of these questions, but I will address the first one, which also relates to the problem of error.

Smart CCTV in public areas is successful, by the standards of both police and manufacturers, when it results in the arrest of a significant number of wanted offenders without at the same time producing large numbers of false positives ("errors") which result in the stopping and questioning of innocent citizens. While Smart CCTV has performed very well in controlled circumstances, it seems that the current technology has not been successful in actual use. In August 2003, the Tampa police force decided to suspend using the system, two year after it was installed, because it had yielded not one arrest or positive identification. ``It's just proven not to have any benefit to us," said Capt. Bob Guidara, a department spokesman. The system in use at Virginia Beach has, likewise, not resulted in any arrests so far (Kopel and Krause, 2002). Yet, as mentioned before, the system in Tampa had already yielded several false positives during its first few weeks in usage.

An article by investigators Kopel and Krause of the Independence Instute suggests that the reason for its failure may be that the technology is not yet up to being used in real-life circumstances: a trial at a security checkpoint at Palm Beach Airport resulted in 1,081 false alarms in a four-week period while people in the database were only stopped 47% of the time (Kopel and Krause, 2002). The problem of error hence still seems to loom large for Smart CCTV. I conclude that the use of Smart CCTV in public places still faces major problems. The problem of function creep is still unresolved, largely because of the absence of clear legislation. The problem of error is also unresolved, because the current technology seems to yield many false positives and few, if any, true positives. And privacy concerns with the technology cannot be sidestepped by reference to the importance of the technology in providing security, because the technology appears to be unreliable as of yet, nor has it been demonstrated that there are no alternatives available.

NOTES

1. All information on Identix and the Faceit system in this section has been taken from Identix' website, www.identix.com, in 2003, and from its predecessor's website, www.visionics.com, in 2001, unless indicated otherwise. The views expressed and conclusions drawn in this and other sections are my own and not those of Identix corp. FaceIt® is a registered trademark.
2. Sources: www.visionics.com; O'Harrow

(2001a, 2001b); Technews.com.

3. According to a Visionics/Identix press release, Keflavik airport in Iceland has been the first airport to use the technology. Others that have followed include Boston's Logan, Dallas-Fort Worth International and Palm Beach International. See also Kopel and Krause (2002).
4. The use of Smart CCTV in stores is relatively rare. The U.K. bookstore chain Big Borders was piloting its use in its stores to catch shoplifters, but the pilot was ended after protests by human rights organizations. See 'Big Borders bookshop is watching you,' *Sunday Herald* (August 26, 2001).
5. See www.identix.com and 'Ybor police cameras go spy-tech', St.-Petersburg Times (June 30 2001).
6. See www.identix.com and 'Surveillance Cameras Incite Protest', *New York Times*, (July 16 2001).
7. 'Tampa Face-Recognition Vote Rattles Privacy Group – Update,' *Washington Post* (August 3 2001).
8. 'TV Cameras Seek Criminals in Tampa's Crowds,' *New York Times* (July 4 2001).
9. See Visionics (2001b) and Canedy (2001).
10. 'Anger over face-scanning cameras,' BBC News, August 20.
11. LEAA statement, US Newswire (July 3 2001). See http://www.notbored.org/leaa.html
12. See Blum (2001a). The Rand report even makes the argument that Smart CCTV can benefit privacy because it is not physically invasive like some other forms of surveillance. See also Woodward (2001).

REFERENCES

Amato, I. (2001) Big Brother Logs On, *Technology Review*, September. http://www.technologyreview.com/articles/amato0901.asp.

Bergstein, B. (2003) Next level in passport technology may not be ready, Associated Press, August 24. 'Your ID Going Digital,' *Cnews Canada*, June 11.

Blum, A. (2001a) Beach may scan Oceanfront faces, *The Virginian-Pilot*, July 6.

Blum, A. (2001b) Va. Beach mayor opposes plan to scan faces, The *Virginian-Pilot*, July 10.

Canedy, D. (2001) Tampa Scans the Faces in *Its Crowds for Criminals, New York Times*, July 4.

Greene, T. (2001) Think tank urges face-scanning for the masses, *The Register,* August 13. http://www.theregister.co.uk/content/6/20966.html .

Herdy, A. (2001) Ybor Police Cameras go Spy-Tech'., *St. Petersburg Times*, June 30.

Hes, R., Hooghiemstra, T. and Borking, J. (1999) *At Face Value – On Biometrical Identification and Privacy.* Registratiekamer, September. http://www.cbpweb.nl/downloads_av/AV15.pdf

Kasindorf, M. (2001) Big Brother cameras on watch for criminals. *USA Today* (August 2 2001).

Kopel, D. and Krause, M. (2002) Face the Facts – Facial recognition technology's troubled past – and troubling future. *ReasonOnline*, http://www.reason.com/0210/fe.dk.face.shtml.

Lyman, J. (2001) Critics Blast U.S. Ties to 'Snooper Bowl' Technology, *NewsFactor Network*, August 2.

Meares, R. (2001) Nowhere to hide, Video Eyes are Watching, *Reuters*, May 24.

Mieszkowski, K. (2001) Stop the webcams, we want to get off! www.salon.com, 28 August.

Nissenbaum, H. (1998) Protecting Privacy in an information age: The problem of privacy in public. *Law and Philosophy*, 17: 559–596.

O'Harrow, R. Jr. (2001a) Facial ID Systems Raising Concerns About Privacy. *Washington Post,* August 1.

O'Harrow, R. Jr. (2001b) 'Matching Faces With Mug Shot. *Washington Post,* July 3 1

Visionics Co. (2001a) O'Rourke Group, Major Civil construction Firm, Deploys Visionics' FaceIt Technology at Main UK Concrete Production Site. *SMN Newswire*, March 22. [Press release]

Visionics Co. (2001b) Tampa Police Department installs Visionics' FaceIt Technology in anti-crime CCTV initiative, Press release, June 29.

Woodward, J. D. (2001) *Super Bowl Surveillance: Facing Up to Biometrics*. Santa Monica, CA: RAND, IP-209.

Corresponding Author

Philip Brey
Department of Philosophy,
University of Twente,
7500 AE Enschede,
The Netherlands
Email: p.a.e.brey@utwente.nl