



# Urban Surveillance and Panopticism: will we recognize the facial recognition society?\*

Mitchell Gray<sup>1</sup>

---

## Abstract

This paper explores the implementation of facial recognition surveillance mechanisms as a reaction to perceptions of insecurity in urban spaces. Facial recognition systems are part of an attempt to reduce insecurity through knowledge and vision, but, paradoxically, their use may add to insecurity by transforming society in unanticipated directions. Facial recognition promises to bring the disciplinary power of panoptic surveillance envisioned by Bentham - and then examined by Foucault - into the contemporary urban environment. The potential of facial recognition systems - the seamless integration of linked databases of human images and the automated digital recollection of the past - will necessarily alter societal conceptions of privacy as well as the dynamics of individual and group interactions in public space. More strikingly, psychological theory linked to facial recognition technology holds the potential to breach a final frontier of surveillance, enabling attempts to read the minds of those under its gaze by analyzing the flickers of involuntary microexpressions that cross their faces and betray their emotions.

---

## Introduction - Urban Insecurity and Surveillance

Urban spaces, both private and public, are increasingly fitted with surveillance cameras, but the spread of closed circuit television may be insufficient to address fears of terrorism and crime in urban settings. Why settle for cameras that see people, when cameras could recognize the people they see? This paper examines facial recognition surveillance mechanisms as a reaction to perceptions of insecurity in urban spaces. Facial recognition systems are tools for detecting and sorting out suspected dangerous persons in the urban environment and reducing fear through the collection of knowledge. They magnify and sharpen vision and awareness, with the hope that observers will be able to see a threat before it can become reality. But seeking to protect society from insecurity with the pervasive gaze of facial recognition may generate heretofore-unimagined insecurities.

It is rapidly becoming an urban instinct to grasp at security through surveillance and knowledge, but this, paradoxically, may add to urban insecurity in a fundamental way: by transforming society in unforeseen directions. There is a threshold point in urban

---

\* The author is indebted to Elvin Wyly, Assistant Professor, Department of Geography, University of British Columbia, for invaluable input.

<sup>1</sup> Freelance journalist, Vancouver, British Columbia, Canada. <mailto:mitchellgray@fastmail.fm>

surveillance beyond which quantitative change - the addition of devices used and areas watched - becomes qualitative change. It follows that we might not recognize the facial recognition society.<sup>2</sup> In *Discipline and Punish*, Michel Foucault highlighted the transformative, disciplinary potential of surveillance, explaining the power inherent to the acts of information collection and analysis. Facial recognition software, with its ability to digitally archive a limitless gaze over urban space, represents a leap in this disciplinary influence.

There is no limit to how completely facial recognition may permeate society as its underlying technologies continue to develop. One cannot assume that traditional conceptions of privacy would have meaning in a society riddled with facial recognition cameras. And it is not just privacy that could be affected; fundamental ways in which members of society interrelate are also vulnerable to change. It is vital to contemplate how those within would experience this type of surveillance-saturated urban environment, and how it could alter urban life.

This paper proceeds through four main sections. First, facial recognition surveillance is defined, highlighting the significant advance it represents over other forms of surveillance. Second, I explore general background issues relevant to surveillance. The third section highlights the transformative potential of facial recognition surveillance with an overview of the “panoptic” tradition of thought and its disciplinary power. It also contemplates the manner in which facial recognition surveillance relates to governance based on risk management. The final section of the paper explores the technology’s potential ramifications, especially in the realm of privacy. It also considers how facial recognition systems may affect those who are observed. The conclusion addresses ways in which societies that value the balance between privacy and security must respond.

## Facial Recognition Defined

Facial recognition programs are part of the growing realm of biometrics, or body measurement. Face images, fingerprints, hand geometries, retinal patterns, voice modulations and DNA are all identification sources unique to individuals. Facial recognition software maps details and ratios of facial geometry using algorithms, the most popular of which results in a computation of what is called the “eigenface,” composed of “eigenvalues” (Selinger and Socolinsky, 2002).

Many basic uses of facial recognition technology are relatively benign and receive little criticism. For example, the technology can be used like a high-tech key, allowing access to virtual or actual spaces. Instead of presenting a password, magnetic card or other such identifier, the face of the person seeking access is screened to ensure it matches an authorized identity. This eliminates the problem of stolen passwords or access cards. In heightened security situations, facial recognition could be used in conjunction with other

---

<sup>2</sup> David Lyon has called modern Western societies “surveillance societies.” Facial recognition may have implications significant and unique enough to warrant the addition of “facial recognition society” to the lexicon. See Lyon, 2001.

forms of identification (Lyon, 2001: 75). The next step in facial recognition is to connect the systems to digital surveillance cameras, which can then be used to monitor spaces for the presence of individuals whose digital images are stored in databases. Images of those present in the spaces under watch can also be recorded and subsequently paired with identities. Surveillance power grows as various systems, public and private, are networked together to share information.

Facial recognition may create economic savings. Policing efficiency could be improved if tracking of suspected terrorists and criminals were automated, for example, and welfare fraud would be curtailed if individuals were prevented from assuming false identities (Etzioni, 1999: 103-105). The potential benefits of facial recognition systems also extend well beyond the realm of crime, terrorism and finances. The software could, for example, help ensure that known child molesters are denied access to schoolyards (Woodward, 2002).

Facial recognition technology requires further development, however, before reaching maximal surveillance utility.<sup>3</sup> The American Civil Liberties Union explains: “Facial recognition software is easily tripped up by changes in hairstyle or facial hair, by aging, weight gain or loss, and by simple disguises.” It adds that the U.S. Department of Defense “found very high error rates even under ideal conditions, where the subject is staring directly into the camera under bright lights.”<sup>4</sup> The Department of Defense study demonstrated significant rates of false positive test responses, in which observed faces were incorrectly matched with faces in the database. Many false negatives were also revealed, meaning the system failed to recognize faces in the database. The A.C.L.U. argues that the implementation of facial recognition systems is undesirable, because “these systems would miss a high proportion of suspects included in the photo database, and flag huge numbers of innocent people - thereby lessening vigilance, wasting precious manpower resources, and creating a false sense of security.”<sup>5</sup>

The fact that problems remain in the implementation of facial recognition tools makes the study of this mode of surveillance no less crucial. Its usage will increase as research continues and the technology becomes more accurate and less expensive. There is little limit to the knowledge that could be compiled about an individual’s presence in monitored spaces using a network of facial recognition systems. As the technology advances, the software will effortlessly track individuals moving through urban space, public and private. Any appearance of a person deemed threatening can be set to trigger an alarm, assuming that person’s face has been recorded in a linked database. The

---

<sup>3</sup> For an overview of the technical aspects of facial recognition, see Phillips et al., 2002.

<sup>4</sup> “ACLU Opposes Use of Face Recognition Software in Airports Due to Ineffectiveness and Privacy Concerns,” *American Civil Liberties Union*, 29 Nov. 2002. At: [http://archive.aclu.org/issues/privacy/FaceRec\\_Feature.html](http://archive.aclu.org/issues/privacy/FaceRec_Feature.html) This viewpoint is supported by the Department of Defense study it quoted. See “Facial Recognition Vendor Test 2000 Evaluation Report,” *U.S. Department of Defense Counterdrug Technology Development Program Office*, 16 Feb. 2001, 29 Nov. 2000. At: [http://www.dodcounterdrug.com/facialrecognition/DLs/FRVT\\_2000.pdf](http://www.dodcounterdrug.com/facialrecognition/DLs/FRVT_2000.pdf)

<sup>5</sup> *American Civil Liberties Union*, 29 Nov. 2002 At: [http://archive.aclu.org/issues/privacy/FaceRec\\_Feature.html](http://archive.aclu.org/issues/privacy/FaceRec_Feature.html)

systems represent a significant advance from closed circuit television (CCTV), which requires constant human attention to scan for potential threats.

Facial recognition also has the ability to reach quickly into the past for information, dramatically extending the effective temporal scope of surveillance data analysis. Once an image is included in the database, stored surveillance data can be searched for occurrences of that image with a few keystrokes. Searching videotape for evidence, by contrast, is extremely time-consuming. The process of determining whether a suspected terrorist visited Berlin in 2002, for example, could require watching thousands of hours of videotape from potentially hundreds of cameras. If those cameras operated digital facial recognition systems, and the suspect's face were available in a linked database, the same search could conceivably be executed in a fraction of the time. The next section situates these qualities of facial recognition in the context of surveillance in general.

### Trends in Surveillance

In their “everyday story of video surveillance” in Britain, Norris and Armstrong (1999) estimate that more than three hundred cameras may film an individual on an eventful day, and they list reasons this number will continue to rise. First, arguments that CCTV is not successful in reducing crime are often dismissed summarily in the media as contrary to common sense. Second, when a particular area introduces a CCTV system, it can displace crime into surrounding areas lacking surveillance, causing the latter to adopt systems also. Third, the presence of surveillance systems is argued to make cities attractive to business. Fourth, the systems have proven useful in gathering evidence pertaining to serious crimes like murder, and in helping police allocate resources by viewing the nature of an event before responding (Norris and Armstrong, 1999:205-206). The current trajectory of surveillance is toward omnipresence; more spaces are watched in more ways, capturing information about those within. The focus of this proliferation in recent years has been CCTV, but subsequent sections explore reasons the spread of facial recognition will continue these trends.

Increases in surveillance are accompanied by a series of important related concerns. Facial recognition systems are prey to most common critiques of surveillance (and others unique to it that will be addressed below). In general, all arguments against camera surveillance apply, because cameras are the carrier for facial recognition technology. Most importantly, surveillance systems jeopardize privacy, and the challenge as surveillance grows is to prevent security solutions from evolving into greater threats to the urban fabric than the ones they are meant to solve. Privacy is inherently valuable, serving a crucial function in the development of individuals and groups. Michael Curry explains:

It is in private that people have the opportunity to become individuals in the sense that we think of the term. People, after all, become individuals in the public realm just by selectively making public certain things about themselves. Whether this is a matter of being selective about one's

religious or political views, work history, education, income, or complexion, the important point is this: in a complex society, people adjust their public identities in ways that they believe best, and they develop those identities in more private settings. (1997:688)

To create a group is to erect a boundary of privacy separating members and non-members. It is also only through privacy that the distribution of political power can change. The less powerful require control over ideas and information in order to formulate an empowerment strategy (Curry, 1997:688).

Like other surveillance tools, facial recognition systems share the problems that arise from secrecy of implementation and the possibility of data errors. Urbanites often remain unaware they are being observed and even when aware, they generally have no access to information collected and therefore no ability to correct erroneous data. The most egregious case of mistaken data in facial recognition terms is pairing a facial image with the wrong identity. Further problems arise when information is networked. Discrete pieces of information about an individual may be relatively harmless to privacy, but when information is shared, a comprehensive dossier on the individual can be assembled. Privacy advocates complain that information ostensibly collected for a specific purpose is frequently used in a myriad of ways, most of which have not been consented to by the subject. This situation becomes more complex and delicate when public and private institutions share information. The ethical issues of governments purchasing information from private entities, which may or may not follow the collection guidelines approved by a democratically elected government, are complex and only slowly being examined.

As the spaces of surveillance grow, private space shrinks. It must be asked whether the potential security and public safety gains from facial recognition systems outweigh the costs to privacy incurred by their use. Healthy societies seek a balance. Drawing the policy line too close to the public safety end of the spectrum could result in an undesirably restricted and unnecessarily transparent society. Conversely, to unconditionally favour privacy could maintain security vulnerabilities at an unacceptable level.

The effects of pervasive surveillance stretch beyond issues related to privacy. At risk, for example, is an erosion of the benefits of routine urban social interaction. Surveillance saturation could cause a shrinking perception of accountability among those present together in urban space. Hille Koskela explains that “electronic means have more and more often [been] used to replace informal social control in an urban environment: *the eyes of the people on the street* are replaced by the eyes of surveillance cameras” (2002:259). There may be less incentive to assist someone in distress when a camera is viewing the event. Why interfere yourself when you can let the “experts” behind the lens do it? At its most essential level, omnipresent surveillance simply has the power to reduce quality of life. Conservative *New York Times* columnist William Safire (2002) describes succinctly how constant surveillance is experienced: “To be watched at all times, especially when doing nothing seriously wrong, is to be afflicted with a creepy feeling .... It is the pervasive, inescapable feeling of being unfree.”

Despite the above concerns, support for surveillance in many Western states and elsewhere is growing. The next section contemplates the roles facial recognition surveillance may come to play in governance. It examines the trend toward risk management through data collection and the prediction of future threats as a solution to insecurity. It also explores the manner in which members of a society saturated with facial recognition cameras are influenced to internalise the norms and values the cameras are meant to preserve, and thereby come to govern themselves. In this way, the power exerted by facial recognition systems has the ability to fundamentally transform society.

## Disciplinary Panopticism, Risk and Governance

Questions of security and public safety influence profoundly the ways cities are designed and experienced. As Koskela says, “The obsession with security has been claimed to be the master narrative of contemporary urban design” (2002:259). This obsession was reinforced recently, when the September 11, 2001 terrorist attacks on the United States prompted a tilt toward the public safety end of the privacy/security spectrum and a centralization of power in many Western societies. Facial biometric surveillance is increasingly sought after in these countries as they reel from newfound perceptions of vulnerability ushered in with the terrorists’ actions. Potential future drawbacks of a facial recognition society are at risk of being ignored or viewed as irrelevant compared to the immediate threat of further terrorist attacks.

The period after September 11 has reinforced Richard Ericson and Kevin Haggerty’s assertion that some Western states represent “risk societies” that “focus on danger, and the perpetual doubt that danger is being counteracted...” (1997:86).<sup>6</sup> The provision of security is the main goal of governance in a risk society, but security is intangible, based only on probabilities. Risk management entails working with probabilistic statements and attempting to increase their certainty. Members of this imagined risk society attempt to tame an unknown future with knowledge and technology, but regardless of the depth of their knowledge and technological prowess, unexpected outcomes arise, leading them to seek ever more perfect knowledge of risk (Ericson and Haggerty, 1997:6). As Reg Whitaker asserts, “[t]he informational appetite of risk aversion seems indefinitely expandable” (1999:45). Dramatic and fearful events like the terrorist attacks of September 11 (and other recent attacks) aggravate the risk society, making more vivid and manipulable the perceptions of risk already present in many societies and strengthening the support for surveillance-based methods of risk management.

Michael McCahill (1998) explains that the management of risk involves regulating people with the goal of reducing insecurity. It represents a transition from reactive social control that operates after rules have been contravened, to proactive strategies seeking to minimize opportunities for crime or terrorist behaviour in the future through the prediction of sources of insecurity. It is also linked to a transition from a concern with issues of the mind, such as criminal motivation, to issues of the body, like observable

---

<sup>6</sup> Ericson and Haggerty built upon the work of Ulrich Beck. See Beck, 1992.

behaviour. According to McCahill, this transition has “given rise to strategies of control which instead of trying to change the individual offender, aim to alter the physical and social structures in which individuals behave” (1998:54).

Risk management is able to enhance security by cataloguing and analysing observable behaviour, but it also has a deeper significance: the ability to directly affect that behaviour. For Foucault (1994), the modern “art” of governance arose with a turning away from the blunt forces of sovereign power and control over a state to a disciplinary influence on the population within a state through the acquisition of knowledge and conduct of analysis about that population. Clive Norris and Gary Armstrong (1998:7) list three types of power created by surveillance. First is a direct, authoritative response seen, for example, when a security guard using CCTV observes a person behaving inappropriately and asks the person to cease the behaviour. The second form is deterrence, exemplified by an individual who refrains from inappropriate behaviour due to a fear of being caught based in the perceived ability of CCTV monitors to identify him. The third form is not meant to punish or deter, but to “abolish the potential for deviance.” This requires an internalisation of the power of surveillance that transforms those under its gaze. Understanding this third type of power begins with Jeremy Bentham’s eighteenth-century disciplinary concept of the panopticon.

The panopticon is a simple architectural design meant to impose order on the lives of those within, be they criminals, insane, workers or school children. A multi-level circular building surrounds a central observation tower. The building is divided into individual cells traversing its entire width, so that sunlight from a window in the outside wall of the cells illuminates each inhabitant for viewing by disciplinarians in the tower. Windows on the tower are fitted with blinds or other mechanisms, allowing disciplinarians to observe those sequestered in the cells without being seen themselves (Foucault, 1995:200). The surveillance ability from the tower is complete: “each actor is alone, perfectly individualized and constantly visible. The panoptic mechanism arranges spatial unities that make it possible to see constantly and to recognize immediately” (Foucault, 1995:200).

The strength of the panopticon derives from the visible yet unverifiable operation of power within. Captives constantly sense the presence of the tower and the possibility they are being observed at any given time, yet have no way to determine exactly when they are under scrutiny (Foucault, 1995:201). In this way, the panopticon induces “in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power” (Foucault, 1995:201). Carefully orchestrated power of this sort does not need to be exercised constantly, because subjects internalise the power relationship. As Foucault explains:

He who is subjected to a field of visibility, and who knows it, assumes responsibility for the constraints of power; he makes them play spontaneously upon himself; he inscribes in himself the power relation in which he simultaneously plays both roles; he becomes the principle of his own subjection. (1995:202-203).

In a similar vein, Norris and Armstrong note that “the power of surveillance is not merely that it is exercised *over* someone but *through* them ....” and “[s]urveillance therefore involves not only being watched but watching over one’s self.” The result is “habituated anticipatory conformity” and social control that automatically enforces commonly accepted societal norms and values (1998:5-6).

An urban space permeated with facial recognition systems is the apotheosis of the panopticon. While CCTV has the power to “see constantly” like the panopticon, only facial recognition can “recognize immediately.” Disciplinary influence can be achieved in this way over bodies on the move; bodies no longer need to be physically sequestered for panoptic discipline to affect them. New dangers lurk in the contemporary panopticon. As surveillance spreads throughout society and its control disperses accordingly, its influence is also dispersed, and in unanticipated ways.

The operation of surveillance power stems largely from its ability to sort and categorize. David Lyon calls contemporary panopticism the “phenetic fix.” It acts “to capture personal data triggered by human bodies and to use these abstractions to place people in new social classes of income, attributes, habits, preferences, or offences, in order to influence, manage, or control them” (2002). Little is known about the overall effects of the process on urban centres and their liveability, and it must be analysed critically. As Lyon says, “We simply do not understand ... the full implications of networked surveillance for power relationships, or of the ‘phenetic fix’ for security and social justice” (2002).

Michael McCahill illuminates the seeds of a problem inherent to phenetic sorting as demonstrated in the British CCTV experience. He contends that surveillant sorting raises the spectre of the destruction of democratic space, describing the fear that “public spaces will increasingly be replaced by pseudo-public spaces like those in shopping malls, where commercial imperatives dominate and what goes on, and who participates, is intensely regulated and tightly controlled so that profitable consumption is maximised” (1998:52). McCahill notes that surveillance systems in Britain have been used frequently to sort out and displace groups such as teenagers or homeless who present no greater threat than making a shopping area less inviting to families or displeasing visitors to a city (1998:51-52).

Part of the debate concerning how these phenetic influences will be managed in the facial recognition context focuses on who is included in the databases the software checks for matches. There is a broad continuum of possibilities. The databases may include only known criminals whose faces have been recorded in strict accordance with legal conditions (for example, the Fourth Amendment in the U.S. Constitution). Or, it could be broadened to include any suspicious person (as has been witnessed after September 11). Depending upon how risk is characterized in society, the list of suspicious individuals may be succinct or extensive. In the extreme, it could be made to include the broadest range of citizens possible.

Certain aspects of the technology make the question of database inclusion moot, however. The facial recognition software may scan urban spaces for criminals, but the cameras record all faces. As Clyde Wayne Crews Jr. (2002) of the libertarian Cato Institute asserts, many “doubt governments can be trusted to discard incidental data collected on innocents.” If the tapes are stored, any face can be added to the database and then a search made retroactively for their presence at a certain location or in general. Governments may find the populace quite willing to allow storage of the information, especially in areas deemed critical for national security. After all, it may be argued, would it be prudent to discard information that might at some point in the future hold clues about a terrorist attack or clues that could help stop one?

There is no assurance that even surveillance information stored for legitimate and justifiable purposes might not fall into the wrong hands or be used inappropriately by authorized information gatherers. Koskela (2002:265) cites an instance in which security camera operators at an Australian casino edited visual events captured over four years onto a videotape they showed at parties. The tape included embarrassing and incriminating events, including couples copulating and individuals urinating. Facial recognition technology could enable enemies, political opponents, or simple publicity seekers to create a personal “blooper” reel on anyone surveillance tapes have captured. Even if a government declares its intention not to share information it collects between departments or with the private sector, these sentiments can change depending on how the risk society becomes aggravated. Additionally, governments have been known to release information unintentionally. An October 2002 audit “revealed that the [U.S.] Navy had lost nearly two dozen computers authorized to process classified information” (Moss and Fessenden, 2002).

The role of surveillance in governance and risk management, and its deeper disciplinary influence, lead to another vital set of questions. How will lives be altered by the experience of living in a facial recognition society? In other words, how will observation directly affect the observed? Simplistic attempts have been made to examine facial surveillance proliferation issues by beginning with the society in which we live and grafting a more extensive hypothetical complex of facial recognition systems into the vision. This is insufficient. Surveillance is a project in which watching the world changes the world. Instead of merely adding facial recognition into the current parameters of our society, one must ask what sort of society pervasive facial recognition systems would create, and how the balance of privacy and surveillance would be manifest there.

### **Will We Recognize the Facial Recognition Society?**

The potential effects of ubiquitous surveillance must not be underestimated; being observed fundamentally influences consciousness. In *Being and Nothingness*, Jean Paul Sartre (1957:235-236) gives the example of a man surreptitiously peeking through a keyhole into a bedroom. As the man peers inside, his consciousness is filled with that which he sees. His full concentration and focus is outward to the room, excluding all other thoughts. Suddenly there is a creak in the floorboards behind him, and the man's

consciousness is instantly and radically altered as he realizes he is under surveillance. His thoughts become self-reflective, and he is conscious of himself as a person in the hallway. Repeatedly finding oneself under camera observation will have unforeseeable effects on consciousness.

The issue of “mob mentality” provides one example of the influence represented by the awareness of anonymity or lack thereof. Mob mentality is an escalation of violent or antisocial behaviour exhibited when disruptive individuals form a group. It is, by definition, behaviour induced by feelings of anonymity. Members of a group are more likely to commit inappropriate actions because they believe the resulting blame will be dispersed collectively rather than individualized. Like in Sartre’s keyhole, facial recognition has the potential to disrupt mob mentality as the awareness of being observed highlights the individual conscience. CCTV may help police identify individuals, but the capacity of facial recognition to recognize immediately assists greatly in sorting out individuals.

There are also many possible interrelational consequences of widespread facial recognition surveillance, one of the most fundamental being a loss of the possibility for redemption. Facial recognition has the potential to create a permanent digital record of daily activities, allowing observers the chance to interpret actions and motivations across a lengthy period of time. Mistakes become permanent. “We all assume that there are things about us that others will forget,” Curry explains, “and we are thereby able to feel that we live in a society where there is the possibility of redemption.” He says, “We rely on the possibility of some facts about us drifting out of sight after the passage of time” (1997:688). *New York Times* columnist Peter Lewis adds, “Who among us, over the course of a lifetime, does not have a day or two that we would rather not recall – let alone have the details be retrievable through a key-word search?” (1998:G1) His colleague Russell Baker (1998) also captures the sentiment: “I hear it said that people who have nothing to hide need not fear this strangulating technology of surveillance. And where are they, these people with nothing to hide?”

Facial recognition systems also permit a menacing extension of a classic surveillance problem involving lack of context and the confusion of information and knowledge. Individuals frequently infer things about others based on limited evidence, meaning one action (or piece of information) is erroneously taken as proof that knowledge has been revealed about a person’s character. But accurate categorization based on non-contextualized bits of information is unlikely. Visual information is more prone to cause this mistake and therefore more memorable and disturbing than other media, largely because it is interpreted more frequently as demonstrating what a person “is,” as opposed to other forms of surveillance, which may track what a person buys or does.

When Madelyne Gorman Toogood hit her child in the backseat of a vehicle in September 2002, in an Indiana department store parking lot, it was the video surveillance evidence that ensured many Americans would remember the act for some time.<sup>7</sup> A newspaper story

<sup>7</sup> “Mom: ‘No excuse’ for striking child,” *CNN.com*, 23 Sept. 2002, 1 Dec. 2002. At: <http://www.cnn.com/2002/US/Midwest/09/23/tuchman.toogood.cnn/>

- even if accompanied by a still photograph of the event - could not have the same impact. The video camera gave the public only one piece of information, that Toogood hit her child that day. Many in the audience in turn used that information and felt confident it gave them the knowledge that Toogood is a “bad” person and an unsuitable parent. Toogood was sorted in some viewers’ minds into the category of child hitter, or even child abuser. Details of the situation and legal reaction to the event can be put aside here. The important point is the effects on the woman and her reputation and the ability of these effects to be enhanced by surveillance.

What the pictures could not reveal was the context of the situation, particularly whether or not it was an isolated incident. Consider a similar but hypothetical situation in which a woman repeatedly hits her child. Imagine also that the woman was in the midst of the most stressful period of her life at the moment and the child was having serious disciplinary problems. And imagine the woman never having hit her child before and being overwhelmed with grief immediately after the incident. She may also have foresworn corporal punishment in the future and vowed to live every moment repaying the child for her one (albeit serious) parenting mistake. The camera shows none of this. In the surveillance society, one action can categorize, or phenetically fix, an individual. Such actions can be searched for in the facial recognition society with a few keystrokes the moment a person develops an enemy or someone who seeks to influence him. The power of surveillance and the categorizing phenetic fix threaten to create a blackmail society.

Society is entering a new frontier of surveillance with digital scrutiny of our faces. Perhaps only surveillance of our thoughts is more intrusive and raises greater opportunities for control and influence, and facial recognition systems represent one step down that path. Current research blurs the boundary between biometrics and mind reading. Even Winston Smith, the ill-fated protagonist in Orwell’s (1983) hyper-surveillant *Nineteen Eighty-Four*, could protect himself from the penetrating gaze of Big Brother’s omnipresent telescreens by maintaining a neutral expression, not allowing his face to hint at signs of inner turmoil and rebellion. This option may no longer be possible, because the face gives clues to our thoughts regardless of how well we discipline our features.

Malcolm Gladwell (2002) chronicled psychologist Paul Ekman’s exploration of involuntary facial “microexpressions” that reveal emotional states. “When we experience a basic emotion,” Gladwell wrote, “a corresponding message is automatically sent to the muscles of the face.” The message is registered there for a “fraction of a second.” In some cases it can be detected only with electrical sensors, but in others it is visible. One common involuntary expression is well known: we recognize a false smile because it does not include the involuntary tightening of muscles around the eyes that accompanies genuine emotion (and which is very difficult to achieve voluntarily). Ekman’s research has drawn attention from the U.S. Defense Advanced Research Project Agency (DARPA), the C.I.A. and the F.B.I. He and colleague Mark Frank are exploring ways facial signals could be used to counter terrorism (Gladwell, 2002). Salk Institute neurobiologist Terry Sejnowski envisions the development of an airport security system

that identifies telltale movements around the lips while a subject answers questions. Travellers could step into an automated kiosk, respond to computerized questioning, then board the aircraft unless the system flags their facial responses as unusual (Ehrenfeld, 2003).

Microexpression-related technology is in its infancy, and as MSNBC journalist Temma Ehrenfeld (2003) cautions, the human psychological construction is complex, and analysts must be cautious to interpret microexpressions as clues, rather than hard evidence. She suggests a man accused of murdering his wife may exhibit microexpressions of happiness in court, but further investigation must be conducted before judging whether he is pleasurably recalling the murder or reminiscing his beautiful honeymoon with his beloved, departed wife. In the airport scenario, security analysts must guard against mistaking travel-related anxiety for secret terrorist plotting.

The above examples demonstrate that facial surveillance proliferation can have extensive individual and interactional results in society, and it is all the more dangerous because of the insidious way it achieves legal support. Courts in the United States, for example, determine instances in which citizens are accorded privacy based upon a test of whether there exists a “reasonable expectation of privacy” in that situation. According to a U.S. Supreme Court ruling, there is no reasonable expectation of privacy for our face, which the Court deems highly public (Woodward, 2002). Individual members of society in general had little influence on this decision. As surveillance proliferates and urbanites become accustomed to encountering new levels of observation in their daily lives, their recourse to claims of facial privacy in specific situations slips away. As soon as society becomes accustomed to a type of surveillance, the reasonable expectation of privacy has disappeared. Urbanites have gradually seen many aspects of privacy disappear. Unlike twenty years ago, the watchful eye of the video camera at stores, casinos and many other businesses and government agencies goes almost unnoticed, and drivers submit readily to being photographed while breaking driving laws.

The negative ways in which urban dwellers may experience facial recognition are all the more salient because they are not countered by the feelings of security they are meant to instil. Koskela’s (2002) examination of women’s perceptions of surveillance indicates that facial recognition software, and camera surveillance in general, is failing to quell women’s fears related to the urban environment. Surveillance proponents argue that women harbour greater concerns about their personal safety in urban areas than men do, and therefore gain even more from urban surveillance, but Koskela challenges this notion.

The problem stems from the unverifiability of the presence and character of the observers in a panoptic situation. Bentham praised this as part of the influence of the panopticon as he envisioned it, but it represents a weakness in the modern urban version. Surveillance cameras fail to significantly reduce women’s fears because they do not know who is observing them. Koskela says that in general, “Women are constantly reminded that an invisible observer is a threat.” This is manifest in warnings from police and others to close their curtains tightly, to beware of snoops or “peeping toms.” The problem is

enhanced by the fact that most employees at observation posts are men. A temptation exists to use the surveillance tools for voyeuristic purposes (2002:263-264).

The “placeless and faceless” nature of video surveillance, with or without facial recognition, causes women to doubt its value. Observation rooms are generally hidden, rendering them placeless to those experiencing the surveillance. The observation could be taking place at a distance that would mean those watching would have little or no chance of intervening in a dangerous situation. Furthermore, a facial recognition match on a criminal would be of little immediate benefit to a woman under attack. Facelessness becomes an issue because women cannot see the observers and therefore have no ability to form a perception concerning their reliability and their willingness to help in a troublesome situation (Koskela, 2002:267-268).

Facial recognition systems have the potential to transform urban spaces in undesirable ways that elude the control of city planners, governments and the populace itself. There is also clear evidence that surveillance frequently fails to engender sensations of security in those under its watchful eye, particularly women. And yet increases in surveillance are an essential component of the aggravated risk society, and it is difficult, if not impossible, to find someone who predicts a halt in the progress of the watchful eye. The question, then, is how can the accountability of those who advocate and operate the systems be ensured?

### **Conclusion – Balancing Privacy and Security**

The first step in harnessing the progress of facial recognition tools is to raise public awareness concerning their use and potential consequences. Privacy International presented its 2001 U.S. Big Brother Award for “Worst Public Official” to the City of Tampa “for spying on all of the Super Bowl attendees” with facial recognition. The annual award presents Orwell-inspired statues “to the government agencies, companies and initiatives which have done most to invade personal privacy.”<sup>8</sup> Beyond raising awareness, there must be an active and widespread debate about the consequences of facial recognition systems and the power they give to their controllers. Cindy Cohn, legal director of the Electronic Frontier Foundation (U.S.), says, “If we are going to decide as a country that because of our worry about terrorism that we are willing to give up our basic privacy, we need an open and full debate on whether we want to make such a fundamental change.”<sup>9</sup>

The objective of surveillance studies must be to ensure that people are more than just objects of information. The power of the panopticon is limited by the process of giving those observed a degree of control over, and knowledge of, facial recognition systems. As surveillance systems are implemented, they must be carefully scrutinized to ensure accountability among those who gain power from the systems. Benefits to public safety must be clearly described, and government must justify any secrecy.

---

<sup>8</sup> “The 2001 U.S. Big Brother Awards,” *Privacy International Online*, Privacy International, 20 Nov. 2002 <http://www.privacyinternational.org/bigbrother/us2001/>

<sup>9</sup> As quoted in Moss and Fessenden, 2002.

There are important openings for dissent in the nascent facial recognition society. The U.S. Supreme Court may have denied a right of privacy over facial features, but there is sociological evidence suggesting people observe a customary right to facial privacy. Journalist Malcolm Gladwell (2002) says we tend to focus on audible communication and ignore much of the visual information given in the face, because to do otherwise would “challenge the ordinary boundaries of human relationships.” Gladwell refers to an essay written by psychologist Paul Ekman in which Ekman discusses Erving Goffman’s sociological work:

Goffman said that part of what it means to be civilized is not to “steal” information that is not freely given to us. When someone picks his nose or cleans his ears, out of unthinking habit, we look away ... for Goffman the spoken word is “the acknowledged information, the information for which the person who states it is willing to take responsibility” ... (2002)

Gladwell writes that it is disrespectful and an invasion of privacy to probe people’s faces for information their words leave out. Awareness of the information also entails an obligation, Gladwell says, to react to a message that was never intended to be transmitted. “To see what is intended to be hidden, or, at least, what is usually missed,” Gladwell explains, “opens up a world of uncomfortable possibilities” (2002). Ideas such as these, that examine the forms of interaction a facial recognition society would create, can be exploited in mounting a defence against the observation onslaught. They may be of little consequence now, when people have yet to experience the full brunt of facial surveillance, but as its drawbacks become increasingly apparent, the arguments will become more salient.

Paradoxically, it may be precisely the potential for surveillance to influence behaviour that may ultimately destroy the possibility of exercising that influence. As panoptic surveillance continues to cover more of the urban space and be experienced more constantly and intrusively by urban dwellers, there is a theoretical threshold point beyond which the surveillance ceases to achieve control. If most members of a society develop the expectation that their mistakes and indiscretions have been recorded and may be revealed, the stigmatisation of their behaviour that encourages orderliness will slowly disappear. If an individual can no longer anticipate that his life - especially the rough edges - is safely hidden from view, there is less incentive for that person to maintain the false distinction between his actual and reported behaviour. Society would gradually adopt new norms, ones that less strictly censure behaviours that were previously common yet concealed. Criticism could be pre-empted at this stage by embracing publicly our foibles and declaring them normal before society at large can say otherwise. It is the same model used by the politician who calmly discloses that he has smoked marijuana with a “Who hasn’t tried it?” tone in his voice.]

Left alone, the trajectory of facial recognition surveillance could result in dramatic changes in individual access to privacy and group interaction. Powerful forces, especially governments but also marketers and others, seek to weaken privacy provisions, even at

the risk of the potentially negative changes this could entail. This is not a new situation, but these institutions and individuals were dealt a favourable hand when the September 11 terrorist attacks aggravated the risk society and facilitated the manipulation of the public consciousness. Only by actively engaging in the ongoing debate between privacy and security advocates immediately, before facial recognition systems are omnipresent, can the evolution of surveillance be balanced with society's need for privacy. Raising awareness of dangers, speculating on the future and taking small steps of resistance is a beginning.

## References

### *Print Material*

- Baker, R. (1998) Quiet, quiet, louie, there's a bug in that martini olive. *New York Times* 13 Feb.
- Beck, U. (1992) *Risk Society: Towards a New Modernity*, trans. Mark Ritter. London: Sage Publications.
- Curry, M.R. (1997) The digital individual and the private realm. *Annals of the Association of American Geographers* 87.4: 681-699.
- Eisenberg, A. (2002) With false numbers, data crunchers try to mine the truth. *New York Times* 18 July.
- Ericson, R.V. and K.D. Haggerty. (1997) *Policing the Risk Society*. Toronto: University of Toronto Press.
- Etzioni, A. (1999) *The Limits of Privacy*. New York: Basic Books.
- Foucault, M. (1995) *Discipline and Punish: The Birth of the Prison*. 1975. New York: Vintage Books.
- Foucault, M. (1994) Governmentality. In James D. Faubion (ed.) *Michel Foucault: Power*. Vol. 3. Essential Works of Foucault 1954-1984 Series. New York: The New Press, 201-222.
- Koskela, H. (2002) Video surveillance, gender, and the safety of public urban space: 'Peeping Tom' goes high tech? *Urban Geography* 23.3: 257-278.
- Lewis, P.H. (1998) Forget Big Brother. *New York Times* 19 March: G1.
- Lyon, D. (2001) *Surveillance Society: monitoring everyday life*. Philadelphia, PA: Open University.

McCahill, M. (1998) Beyond Foucault: towards a contemporary theory of surveillance. In Clive Norris, Jade Moran and Gary Armstrong (eds.) *Surveillance, Closed Circuit Television and Social Control*. Aldershot: Ashgate, 41-65.

Norris, C. and G. Armstrong (1998) Introduction: power and vision. In Clive Norris, Jade Moran and Gary Armstrong (eds.) *Surveillance, Closed Circuit Television and Social Control*. Aldershot: Ashgate, 3-18.

Norris, C. and G. Armstrong (1999) *The Maximum Surveillance Society: The Rise of CCTV*. Oxford: Berg.

Orwell, G. (1983) *Nineteen Eighty-Four*. 1949. New York: Penguin Books.

Sartre, J.P. (1957) *Being and Nothingness; an essay in phenomenological ontology*. Trans. Hazel E. Barnes. London: Methuen.

Whitaker, R. (1999) *The End of Privacy: How Total Surveillance is Becoming a Reality*. New York: The New Press.

#### *Electronically-Sourced Material*

Crews, C.W. Jr. "Human Bar Code." Cato Institute. 1 Nov. 2002. 24 Nov. 2002  
<http://www.cato.org/cgi-bin/scripts/printtech.cgi/research/articles/crews-021104.html>

Ehrenfeld, T. "What's in Your Face." *MSNBC News Online*. 9 June 2003. 20 June 2003  
<http://stacks.msnbc.com/news/920497.asp?cp1=1>

Gladwell, M. "The Naked Face: Can you read people's thoughts just by looking at them?" *gladwell.com*. 29 Nov. 2002 <  
[http://www.gladwell.com/2002/2002\\_08\\_05\\_a\\_face.htm](http://www.gladwell.com/2002/2002_08_05_a_face.htm)

Lyon, D. "Surveillance Studies: Understanding visibility, mobility and the phenetic fix." *Surveillance and Society* 1.1. 15 November 2002  
<http://www.surveillance-and-society.org/articles1/editorial.pdf>

Moss, M. and F. Fessenden. "New Tools for Domestic Spying, and Qualms." *New York Times* 10 Dec. 2002. 11 Dec. 2002  
<http://www.nytimes.com/2002/12/10/national/10PRIV.html>

Phillips, P.J. et al. "An Introduction to Evaluating Biometric Systems." U.S. Department of Defense Counterdrug Technology Development Program Office. 29 Nov. 2002  
<http://www.dodcounterdrug.com/facialrecognition/DLs/Feret7.pdf>

Safire, W. "The Great Unwatched." *New York Times* 18 Feb. 2002. 12 December 2002  
[www.nytimes.com/2002/02/18/opinion/18SAFI.htm](http://www.nytimes.com/2002/02/18/opinion/18SAFI.htm)

- Selinger, A. and D.A. Socolinsky. "Appearance-Based Facial Recognition Using Visible and Thermal Imagery: A Comparative Study." Equinox Corporation. 15 Dec. 2002 [http://www.equinoxsensors.com/publications/andreas\\_face.pdf](http://www.equinoxsensors.com/publications/andreas_face.pdf)
- Woodward, J.D. Jr. "Super Bowl Surveillance: Facing Up to Biometrics." Issue Paper 209. Rand Arroyo Center (Army Research Division). 29 Nov. 2002 <http://www.rand.org/publications/IP/IP209/IP209.pdf>
- "ACLU Opposes Use of Face Recognition Software in Airports Due to Ineffectiveness and Privacy Concerns." American Civil Liberties Union. 29 Nov. 2002 [http://archive.aclu.org/issues/privacy/FaceRec\\_Feature.html](http://archive.aclu.org/issues/privacy/FaceRec_Feature.html)
- "Facial Recognition Vendor Test 2000 Evaluation Report." U.S. Department of Defense Counterdrug Technology Development Program Office. 16 Feb. 2001. 29 Nov. 2000 [http://www.dodcounterdrug.com/facialrecognition/DLs/FRVT\\_2000.pdf](http://www.dodcounterdrug.com/facialrecognition/DLs/FRVT_2000.pdf)
- "Mom: 'No excuse' for striking child." *CNN.com*. 23 September 2002. 1 Dec. 2002 <http://www.cnn.com/2002/US/Midwest/09/23/tuchman.toogood.cna>
- "The 2001 U.S. Big Brother Awards." *Privacy International Online*. Privacy International. 20 Nov. 2002 <http://www.privacyinternational.org/bigbrother/us2001/>