**Living on the Wrong Side of a One-Way Mirror:**
**Face Recognition Technology and Video Surveillance**

Grayson Barber

July 16, 2001

Jersey City has installed video surveillance cameras in public. The City of Tampa used face recognition software to scan every fan attending the 2001 Superbowl. The State of Colorado is scanning driver license photos into a database to match against criminal mug shots on file nationwide. The reported capacity of the technology used in the United Kingdom for general identification and surveillance is 50 million faces per second, roughly the total population of England.

Generalized and passive surveillance can be the condition of life in a tyrannical police state, as memorably portrayed in Orwell's *1984*, or merely the result of gradual desensitization in the United States, where consumer profiling is routine, panoptical television sets are marketed as highly desirable, and people relish the thought of being on television.

**What is Wrong with Surveillance?**

Cast strictly in terms of constitutional law, the legal case against video surveillance and face recognition technology rests on the Fourth and Fifth Amendments, which protect against unreasonable searches and seizures and self-incrimination. These constitutional protections have never been invoked against blanket surveillance of whole populations. Face recognition and video surveillance permit organs of the government to probe and search bad actors and good actors alike, without warrants and without probable cause or individualized suspicion.

There are no federal or state laws that limit the scope of face recognition or video surveillance, that criminally punish those that violate the law or that create enforceable civil remedies for the victims of abuse. There are criminal penalties for and civil remedies for abuses of technology that have become old-fashioned, like wiretapping. But new surveillance technologies are far less heavy-handed, so they seem less intrusive, and they can be adopted incrementally for purposes that, ostensibly at least, are quite beneficial.

There is another great difficulty with mounting legal arguments against face recognition and video surveillance technology, and that is the distinction in the United States between the public sector and the private sector. The Constitution places limits only on governmental powers. Accordingly, the Fourth and Fifth Amendments protect against overreaching by the state. When private corporations install cameras and "profile" consumers, Americans perceive no assault on their rights. We have grown accustomed to the presence of hidden cameras in banks and convenience stores. We have adopted the habit of using surveillance for social control, to maintain order and to create a sense of safety and security. With respect to the private sector, our expectation of privacy is almost gone.

Does one have any rights over one's personal "biometric" data: the distance between one's eyes, the slope of the nose, the angle of the cheeks, the thickness of lips, not to mention DNA, fingerprints, and retina scans? There are no laws on the books, and there may be no legal remedies in the courts. Is there nevertheless a right to be free from surveillance in a public place?

In a brilliant essay in the Spring 2001 issue of the journal *Social Research*, Princeton Professor George Kateb makes the case that video surveillance and data mining erode our integrity as individuals. When the world is divided between those who watch and know, and those who are watched and are known, each of us on the wrong end of the camera is treated like a lab animal:

> One is insulted, and insulted deeply, because one loses all possibility of innocence. … [O]ne is crudely treated as interesting and even as presumptively or potentially guilty, no matter how law abiding one is. … One is placed under constant suspicion just by being placed under constant watchfulness and placed under the implicit interrogation that exists when the accumulated information on oneself is seen as a set of integrated answers that add up to a helpless, unauthorized autobiography. Such a loss of innocence just from these two sources is so massive that the insult involved constitutes an assault on the personhood or human status of every individual. "On Being Watched and Being Known," 68 *Social Research* 269, 274-275 (2001).

**What is Right with Face Recognition Technology?**

There is a lot that is good about biometrics. Properly applied, the technology can reduce fraud. The distinction to be drawn is between access control and identification. To make sure that only authorized people have access to a vault, for example, face recognition might be appropriate. Using an iris scan for access to a sensitive computer makes sense. Maybe even a fingerprint for point-of-sale verification when someone uses a credit card. But using biometrics to identify certain groups of people, even criminals, opens the door to potential abuse. A Tutsi vector would have helped the Hutus in Rwanda.

The proponents of face recognition technology point out that biometrics are no worse than human security guards. People practice unconscious discrimination, holding preconceived notions or stereotypes about other people. Biometrics are neutral, they say,

and face recognition scans for known criminals (or other undesirables). The data don't support this assertion, however. The young, the male and the black are systematically and disproportionately targeted. Data from the UK suggest that when the men who conduct video surveillance train the cameras on women, the footage of breast shots and buttocks reek of voyeurism. There is every reason to believe that police will use technology to monitor those who they think are more likely to commit crimes.

Is there adequate evidence that video surveillance or biometrics reduce crime? The face recognition technology at the Superbowl would not have prevented the bombings at Oklahoma City, the World Trade Center or the Atlanta Olympics. School shootings have all to often been captured on the schools' video surveillance cameras. We don't have enough data to know whether surveillance technology actually makes the world a safer place.

Nor are health and safety the only dubious justifications offered for surveillance. Colorado says it needs a photo database of every driver in the state to prevent fraud. No doubt there is a market for counterfeit drivers licenses. But does this justify the expense of creating the photo database of every driver? Colorado already sells driver records to insurance companies for $5 million per year. Surely the photo database will be useful for other commercial, marketing or law enforcement purposes.

The company that brought biometrics to the Superbowl, Viisage, has one-third of the market for digital drivers license photos. It markets digital photos for national voter identification cards and immigration cards. At a rate of 50 million faces per second, current technology will permit a government or private entity to monitor the identification and whereabouts of every citizen of a state from second to second.

Viisage says there is nothing private about one's face. I disagree.

**Privacy in Public.**

It is wrong to assume there is a category of information about people that is "up for grabs" for anyone who wants to use it, for which "anything goes." Privacy scholar Helen Nissenbaum calls this the problem of "privacy in public." She points out that the Central Park rape occurred in public, as did the trial of the accused, but the victim maintains a measure of privacy as to her identity. It is within one's rights to say "none of your business" to a stranger who asks your name, even in a public square or sidewalk. It is equally wrong to say that an aggregation of information does not violate privacy if its parts, taken individually, do not.

The Constitution doesn't permit the government to search and search and search until it can find something you may have done wrong. This has not dissuaded anyone from using surveillance technology. Our government, and private enterprise, are putting databases and software in place, not with total domination as a conscious purpose, but as an incremental expansion of power over individuals.