Shot Spotter and FaceIt: The Tools of Mass Monitoring.

by

Christopher Benjamin [1]

I. Introduction

In 1948 George Orwell brought us the story of Winston and his subservience to Big Brother, the so-called institutionalized benefactor who kept the public's best interests in mind by protecting the public from itself. [2] Winston, like the rest of the citizenry, lived in front of telescreens that conceivably monitored every motion and sound. There was no way of knowing whether you were being watched at any given moment. How often the police monitored any individual was a matter of speculation. It was conceivable that the government watched everybody all the time. One thing was certain -- they could watch whenever they wanted to watch. You had to live from habit in the assumption that every thing you did was observed. Winston was fortunate in that the telescreen in his home was in an unusual position. Instead of being placed where it could command the whole room, the telescreen permitted Winston to sit in an alcove out of sight. In this little nook of privacy, Winston sat and opened a diary. The act was not illegal per se, but would surely be punished by death or life in a forced labor prison if detected. This technologically enabled police state probably seemed far-fetched in 1948, but technology has advanced to the point where the realization of such an environment appears all too possible.

Experience, as reflected in case law, has shown that law enforcement has always been willing to exploit technology as far as the letter of the law will allow. The platitude, "The road to Hell is paved with good intentions," immediately comes to mind when one considers technologies like the Shot Spotter and FaceIt facial recognition software. While these technologies on first impression seem like legitimate law enforcement tools, they could quickly become Orwellian ears and eyes--telescreens made for monitoring our public spaces.

At times it is tempting to believe that as American citizens we enjoy a constitutional right

to privacy. No such guarantee exists explicitly in the Constitution – an implied penumbra being the best that we can manage. Even the protection from unreasonable searches and seizures under the Fourth Amendment hinges on the expectations of our society as a whole. The U.S. Supreme Court in *United States v. Katz* held that the Fourth Amendment's right to be free from unreasonable searches and seizures applies to people and not places. [3] The Court also held the Fourth Amendment's requirement for a search warrant only applies to subjective expectations of privacy that the society as a whole would recognize as reasonable or justifiable. Coincidentally, the Court adopted this approach while technological advances were being made in eavesdropping devices.

The purpose of this note is to consider the legality of the Shot Spotter and FaceIt facial recognition software and whether this government exploited technology has moved or blurred the line between what is public and what is private.

II. The Right to Privacy

There is no explicit right to privacy in the U.S. Constitution, but the Supreme Court has found a limited right to privacy based on a jurisprudence of fundamental human rights. [4] The Supreme Court has described this right as a "penumbral right" emanating from the First, Third, Fourth, Fifth, Ninth, and Fourteenth Amendments. [5] The landmark decisions at the core of this penumbra, *Griswold v. Connecticut* [6], *Roe v. Wade* [7], *Whalen v. Roe* [8], and *Bowers v. Hardwick*, [9] were limited to certain rights of privacy and autonomy with regard to intimate life decisions like whether to have children or to engage in consensual sexual relations. [10] Arguably the most explicit grant in the Constitution to be free from governmental intrusions is the Fourth Amendment.

The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly

> describing the place to be searched, and the persons or things to be seized. [11]

One of the primary functions of the Fourth Amendment is to protect innocent citizens' right to privacy. The Fourth Amendment imposes limits on search-and-seizure powers in order to prevent arbitrary and oppressive interference by enforcement officials with the privacy and personal security of individuals. [12] "The overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State." [13] However, "...the Fourth Amendment does not proscribe all searches and seizures, but only those that are unreasonable." [14]

The standard for determining whether a warrant is required has changed significantly in the last century and the advancement of technology has played a major role in shaping the law. Courts used to apply the warrant requirement of the Fourth Amendment rather literally. Searches were conducted when the police trespassed into protected places or seized protected things – persons, houses, papers, and effects. [15] The Supreme Court held in *Olmstead v. United States* that surveillance, in this case a telephone wire tap, did not constitute a search because eyes and ears, even when enhanced by technology, are not capable of trespass or seizing tangible property. [16] The Supreme Court changed its definition of a search in *Katz*, when the police, without a warrant, attached microphones to the exterior of a phone booth in order to gather evidence that an individual was engaged in bookmaking. The government, relying on *Olmstead*, said the action did not constitute a search because nothing was seized and there was no physical invasion of the phone booth.[17] The Court disagreed and held that the Fourth Amendment protects people from warrantless searches when the government invades an individual's expectation of privacy and that expectation is one that society recognizes as reasonable. [18] The most significant element of the rule espoused in Harlan's concurring opinion is determining whether the individual's subjective expectation is one that society recognizes as reasonable.

While this rule allows a great deal of flexibility, it can also be elusive and difficult to apply. "...[W]hat makes an expectation 'reasonable' is itself a social construct, and the

conclusion that a[n]...expectation was or was not reasonable inevitably turns on more detailed and subtle evaluations." [19]

Two subsequent decisions dealing with expectations of privacy are *Oliver v. United States* [20] and *California v. Greenwood.* [21] The U.S. Supreme Court in *Oliver* took one step of many in determining what the boundaries of the public are and where the police may search without a warrant. The Court held that an individual may have a justifiable expectation of privacy in his or her curtilage, the area immediately surrounding one's home, but not an open field.

A person's curtilage or the things within it are not totally free from scrutiny either. In *California v. Greenwood* the defendant placed his garbage, contained in opaque garbage bags, outside to be disposed of by the city's waste disposal service. While the contents of the defendant's garbage may not have been readily apparent to the public, the Court said the expectation was not one society would consider reasonable because anyone could open the bags and examine the contents. [22]

The general rule of thumb arising from this string of decisions is that one may not have a justifiable expectation of privacy in that which they knowingly expose to the public.

III. Technology Pushes the Boundaries

The government, particularly law enforcement, has always been keen to use technology to enhance the visual, auditory, and olfactory senses of its agents in an effort to detect the perpetration of crime. As new technologies are added to the government's arsenal, the courts have been repeatedly asked to balance the interests of the government in maintaining law and order with the elusive and evolving expectations of privacy held by the public. But have the courts' decisions, delineating which methods of surveillance are permissible, only brought the boundaries of the public to our attention or have they expanded the boundaries of the public while diminishing our "zones" of privacy? Perhaps the courts have done both of these things.

The devices used by the government have ranged from the exceedingly low-tech to the

cutting edge. In *United States v. Place* the Supreme Court approved the use of drug-sniffing dogs to inspect luggage, because it was a less intrusive alternative to opening all the bags and society is not prepared to recognize a right of privacy in how luggage smells. [23] Likewise, the Court in *Jacobson v. United States* upheld spot checks for cocaine through chemical analysis of residue found on the exterior of luggage. Again, the Court was unwilling to recognize a right to privacy in the exposed exterior of luggage. [24] Chemical analysis of a paint sample taken from a car left in a parking lot was upheld in *Cardwell v. Lewis* – again, because there was no justifiable expectation of privacy in the exterior or the identity of the car. [25] In *Smith v. Maryland* the Supreme Court upheld the use of a pin register by the police to monitor whom the defendant had contacted via telephone. [26] The Court held that while a person does have a reasonable expectation of privacy in the contents of their telephone conversations, no legitimate expectation of privacy in whom the defendant contacted by phone exists. The Supreme Court in *Florida v. Riley* considered whether surveillance of a greenhouse, located in a residential backyard, from a helicopter hovering at 400 feet constituted a search and held it was not because it was not unusual for helicopters to fly overhead. Therefore, the defendant had no reasonable expectation of privacy. [27] As such, the government may document what they observe from high altitudes through aerial photography, and the "slight" enhancement of human vision does not implicate any constitutional concerns. [28]

Technology continues to advance and the police continue to take full advantage of it. Two recent examples are the Shot Spotter and FaceIt facial recognition software.

IV. Orwellian Ear in the Making?

The Shot Spotter is a product specifically designed for and marketed to law enforcement as an "early warning system" for reporting gunfire. [29] A California-based corporation, Trilon Technology, produces the Shot Spotter. [30] The system consists of a network of microphones, approximately 8 per square mile, positioned on rooftops and telephone poles. [31] The microphones are then fed into a central computer. The microphones pick up the everyday sounds

of the neighborhood, such as car horns, barking dogs, backfiring cars, etc. [32] When a particularly loud acoustic spike is detected, the computer establishes the location of the sound within an area of twenty feet through a mathematical process known as triangulation. [33] The computer basically determines the microphones' relative positions to the gunshot by calculating the difference in time between the individual microphones detecting the gun shot. [34] Upon determining the location, the computer displays where the shot originated on a map of the neighborhood. The process takes the computer seconds to complete. [35] With this information police dispatchers can direct officers to the scene.

Several newspaper descriptions of the Shot Spotter state that the microphones are hidden, which is somewhat misleading. [36] The microphones are elevated for the primary purpose of covering a wide area. Officials have been resistant to disclosing the exact locations of the microphones, fearing that they might become the targets of gunfire. [37] However, the police have recognized that in order for the Shot Spotter to deter people from discharging firearms, then the public must necessarily be aware that the system is there and works. Publicity about the system has intensified since the system was installed. [38] But rather than relying on the media to inform the public of its existence, at least one law enforcement agency has gone so far as to launch a door-to- door campaign to alert residents that the police are able to monitor and locate gunfire. [39]

The Shot Spotter can also be used in conjunction with the automated telephone system Dialogic's Communicator. [40] Once the computer has established the location of the shot, Communicator calls every available telephone number in that area and plays a recorded message such as, "Shots have been fired in your neighborhood. Have you heard anything?" [41] Communicator compiles which homes have been contacted and re-dials the numbers where it received no response. [42] It also records the responses to automated questions about the shooting and has the ability to transfer people to a live dispatcher. [43]

Listening systems have been considered by Cincinnati, Ohio [44] and Oak Cliff, Texas [45] and utilized in: Redwood City, California [46]; Willowbrook County, California [47]; and San Mateo County, California. [48]

Citizens have voiced their concerns that the microphones might pick up conversations. [49] The manufacturer insists that the system's recording capabilities are triggered only by extremely loud, explosive sounds and limited to eight-second intervals. [50] A Trilon spokesman said:

> We aren't interested in anything other than gunfire and we don't listen to anything other than gunfire and we can't hear anything other than gunfire. So it's not an issue of privacy for us. Someone who's shooting a gun in the air, from our perspective, has given up their right to privacy. [51]

Citizens are not the only ones concerned. Van Jones, Executive Director of the Ella Baker Center for Human Rights, has called the technology a slippery slope leading to a camera and microphone on every public street corner. [52] "Then everybody would be safe. But nobody would be free. And that's the danger-- that we're moving in the direction now where we're pushing law enforcement into creating a surveillance security state." [53]

Jeff Chester of the Center for Media Education called the Shot Spotter, "The first visible example that we're creating an infrastructure of surveillance...I think this kind of intrusive technology goes beyond prudent police work. This community eavesdropping is a very dangerous concept." [54]

Constitutional rights attorney Scott Greenwood stated that he doesn't "...believe the government for a moment when it says it would listen only for certain sounds." [55] He added that microphones infringe on the public's ability to engage in activities protected by the Constitution and suggested the money spent on the system would be put to better use by hiring more officers. [56]

Greenwood's criticisms may be valid. While the Shot Spotter may not be presently configured to record conversations, it may be capable of modification for other uses. The computer is programmed to record in response to stimuli from non-discriminating microphones, and computer programs can be altered. One author has envisioned using these listening beacons as a means of detecting other crimes and enforcing intellectual property rights. [57]

The Shot Spotter doesn't lead to many arrests for the unlawful discharging of a weapon. [58] After a year of testing in Redwood City, California, the system alerted dispatchers 66 times. [59] Twenty-one of the reports resulted from gunfire, twelve were from unknown explosions, and fifteen were unidentified. [60] The remaining eighteen reports were not investigated by an officer at all. [61] In Willowbrook, California the Shot Spotter reported nine shootings on a street in less than four months, resulting in only one arrest. [62]

Trilon Chief Executive Officer Bruno Kaiser stated that the Shot Spotter's benefits extend beyond finding people firing weapons, but that the system serves as a deterrent. [63] The primary emphasis by police in Redwood City has been prevention. [64] The general consensus is that the Shot Spotter has reduced the number of random shots fired where utilized, but could it deter people from engaging in constitutionally protected activities like speech?

V. Just Making Conversation

The contents of conversations are precarious. When engaging in conversation, a speaker assumes the risk that the listener will not honor the speaker's expectation of confidentiality and may reveal the contents of the conversation. [65] In *Hoffa v. United States* a government informer went to Jimmy Hoffa's hotel room to gather information. Hoffa, assuming the informer had his best interests in mind, made incriminating statements. The informer was then entitled to testify to Hoffa's statements, because Hoffa's expectation of privacy was not reasonable. The U.S. Supreme Court extended *Hoffa* in *United States v. White* by holding the use of a recording or transmitting device does not bring the Fourth Amendment into play, because all it does is substantiate what the listener would testify to anyway. [66] While the determinative focus on place was deemed misguided by the Supreme Court in *Katz*, place is still a factor to be considered when determining whether a conversation is protected through a reasonable expectation of privacy. [67]

Case law stands for the proposition that the government is listening – and we should be aware of that fact. The Second Circuit in *United States v. Mankani* upheld the technologically unaided eavesdropping of an adjacent motel room, reasoning that it was not a search when an

officer is lawfully present at a certain place and detects something through his natural senses. [68] Moreover, *U.S v. Agapito* held that an agent could lawfully stand with his ear pressed against an adjoining hotel wall and that such action could be reasonably anticipated by the occupants. [69] The *Agapito* court reiterated the stance taken in *United States v. Llanes* in which the Second Circuit permitted the police, who were standing in a hallway, to testify to overheard statements made by a defendant while in his apartment. [70]

> [A]n individual who speaks in a tone audible to a person outside his door does not have a reasonable expectation of privacy. Although the defendant expected that conversations spoken in his apartment would be private, his expectation of privacy was not reasonable. He took the risk that the conversations would be overheard by others. We did not consider it onerous to hold the defendant to such a risk, observing that "(t)he risk of being overheard by an eavesdropper. . . is probably inherent in the conditions of human society. It is the kind of risk we necessarily assume whenever we speak." [71]

While *Mankani*, *Agapito* and their underlying precedents dealt with the expectation of privacy in hotel rooms and homes, the expectation of privacy in conversation conducted in public places is more precarious. The *Mankani* court stated, "Just as what an officer sees when lawfully present is considered nonintrusive plain view, what he hears while so stationed is similarly not a search and seizure and is thus per se lawful."[72] "Therefore, there is an accepted loss of privacy when one occupies a public place, *somewhat akin to a conversation in the street*, and the intervention of a human ear in those surroundings is the kind of intrusion one should anticipate." (emphasis added)[73]

Indeed, there appears to be no federal prohibition against electronic eavesdropping in public places like streets or parks. If federal case law offers no protection against eavesdropping on publicly held conversation, federal statutes offer no alternative refuge. Title III of the Omnibus Crime Control and Safe Streets Act of 1968 regulates the technological interception of wire, electronic and oral communications. Oral communications is defined by Title III as, "...any oral communication uttered by a person exhibiting an expectation that such communication is

not subject to interception under circumstances justifying such expectation..." which brings our analysis right back to *Katz*.[74]

A reasonable expectation of privacy in the contents of a publicly conducted conversation may be theoretically possible. In *Katz* Justice Stewart pointed out the key is whether the defendant sought to exclude "the uninvited ear." [75] But how is one to exclude prying ears in public in any practical sense? Even if we are to whisper, the courts may be leery of trying to draw any bright-line rules regarding how the level of one's voice effects expectations of privacy.

> In essence, the [defendants'] argument is that eavesdropping is permissible only when the speaker takes the risk of speaking loudly but not when the speaker uses normal tones audible only to an ear pressed to the door. Granted, the argument has a surface appeal; one who speaks in a normal tone may have a more reasonable expectation of privacy than one who speaks loudly. On the facts of this case, however, we find the argument to be unpersuasive. [76]

In order to keep a statement private, the declarant may be forced to delay uttering what he intends to say until he is indoors – and away from doors, windows and thin walls.

VI. Another Face in the Crowd

The creation and installation of an audio surveillance network like the Shot Spotter can easily be construed as a piecemeal step towards the creation of a telescreen, monitoring the public, when combined with FaceIt facial recognition technology. Surveillance cameras are nothing new to the American public. The first two public uses of video camera surveillance were by the cities of Hoboken, New Jersey, in 1966 and Mount Vernon, New York, in 1971 as a means of improving the crime rate of downtown business and shopping districts. [77] Frequently the use of video surveillance is used to the same extent as the cop on the beat, to prevent and detect crime. [78] More than 60 urban centers in the U.S. use video surveillance in public places for law enforcement purposes. The city of Baltimore, Maryland initiated a program in 1996 with the objective of having 200 cameras monitoring 200 city blocks. [79] The proliferation of video

cameras has caused some to speculate that anonymity in a sea of faces will become a thing of the past. [80] One journalist commented:

> So, as surveillance expands, it has the effect of enlarging the reach of the police. Once it becomes possible to bank all these images, and to call them up by physical typology, it will be feasible to set up an electronic sentry system giving police access to every citizen's comings and goings. [81]

This vision has been realized and is being used. Like so many other technologies developed by the military, face recognition technology has been adopted by law enforcement to monitor the streets and there appears to be no federal impairment barring American law enforcement from doing so.

A company in Jersey City, New Jersey named Visionics Inc. has developed a face-recognition system capable of comparing one photo with millions of photos in a database and selecting a match. [82] The Visionics's program entitled FaceIt mimics the way people recognize faces.

The human brain is bombarded with information, and our brains automatically eliminate redundant information and remember only unique features in order to identify objects or people. [83] FaceIt video cameras capture a face and are fed into a computer which identifies people by their facial features. Visionics concluded there are 80 unique landmarks on a face, which include eye sockets, cheekbones and the bridge of the nose. The computer measures these landmarks and their relationship to one another. Since each face has it own unique pattern, with the exception of identical twins, the computer is able to distinguish one person from another by referencing the person's face against a database of known people. While the program potentially has 80 landmarks to work with, the computer only has to match 14 to make a reliable identification. [84] The software ignores changeable characteristics like: hair color, hair style, lighting, and facial expressions. [85] On May 7, 1999 Visionics announced that their FaceIt surveillance system has been benchmarked at 12 million comparisons per minute. [86]

Mass monitoring via facial recognition technology was first used in England as part of a five-year initiative to reduce crime and anti-social behavior. [87] The police in Newham, a borough of London, have installed 250 closed circuit video cameras through the streets and connected them to the FaceIt system. [88] As pedestrians go about their business, their faces are being scanned and compared to a database of known criminals. When a match is made, the computer alerts law enforcement.

Bob Lack, who manages security technology for the borough of Newham, has stated, "We don't regard ourselves as 'Big Brother.' We're more like a friendly uncle and aunt watching over you." [89]

Joseph Atick, president of Visionics, said the system's real value lies in its deterrent effect. [90] He also stated the facial recognition system strikes a balance between individual privacy rights and society's expectation of public safety. He insisted that law abiding citizens have nothing to fear, as the system will disregard their countenance upon determining their absence from the database. [91]

The system has reduced incidents of crime in Newham and has met with approval from Prime Minister Tony Blair. [92] In fact, Newham has received a grant to upgrade and expand the system as part of a 33 million-pound national closed circuit television camera initiative. [93]

Public mass monitoring through facial recognition technology was first used in the United States in January, 2001 in Tampa, Florida in an effort to shore up security at Super Bowl XXXV. [94] As 100,000 spectators and employees passed through the turnstiles of Raymond James Stadium, each face was compared to a database with over 1,700 known criminals and international terrorists. [95] Super Bowl security used a facial recognition system similar to FaceIt called FaceTrac. [96] After the game the general public was informed of the use of the facial recognition technology to mixed reaction, with the nickname "Snooper Bowl" being coined. [97]

While the arguably exigent circumstances of the Super Bowl as a terrorist target may justify the limited use of facial recognition technology, no such circumstances exist for its continued use. Yet, Tampa Bay has seen fit to continue to monitor the streets of Ybor City, a

night life district, with a 36 camera FaceIt system in place. [98] The Ybor area is one of the city's busiest tourist attractions and is in close proximity with some of the city's high-crime neighborhoods. [99] The City Council passed the motion to implement the FaceIt system without debate or public hearing. [100] The system was implemented as a crime prevention tool, similar to the system in place in Newham, England, but Tampa Bay is also using the system to look for run-away children and to discourage under-age drinking. [101] The police are considering expanding their system to other parts of Tampa Bay.

Jack Walters, a board member of the Tampa Bay chapter of the American Civil Liberties Union (ACLU), said, "This is Big Brother actually implemented. I think this just opens the door to it being everywhere." [102]

Mr. Walters may be right. The city of Virginia Beach, Virginia is seeking a state grant to implement a facial recognition network. [103]

To some extent state governmental bodies are already using facial recognition technology. West Virginia uses a face recognition system to prevent people from acquiring drivers licenses under a fraudulent name. [104] Massachuset's welfare agency uses face recognition software to prevent multiple claims by the same person. [105] The Los Angeles Sheriff's Department caught a mugger by comparing a sketch with 30,000 mug shots in its database. [106] Additionally, the Maryland Department of Public Safety and Correctional Services and Arlington County law enforcement in Virginia have awarded contracts to a leading biometric provider with the intention of combining facial recognition with a mugshot database to aid with the booking process. [107]

U.S. government officials are considering their own uses for this technology. Timothy Biggs, Section Chief of biometrics for the Immigration and Naturalization Service (INS), believes replacing fingerprinting with facial recognition technology would speed up the process of crossing the U.S. border. [108] Brian Wall, Director of the Security Services for the International Air Transport Association, commented that the technology would not only speed up the process of international travel, but would also contribute to its safety. [109]

While these limited uses of facial recognition software go legally unchallenged, American law enforcement appears to be free under federal law to use facial recognition technology to its fullest. The Fourth Amendment is a limitation against unreasonable searches and seizures, but mass monitoring through the use of FaceIt does not rise to the level of a search under Fourth Amendment jurisprudence.

Objections could be made to the use of FaceIt by U.S. law enforcement on the grounds that it invades an individual's expectations of privacy in their face or movements, but those arguments would fail. Coinciding with the rationale in *Katz* that a person has no reasonable expectation of privacy in that which they knowingly expose to the public, the U.S. Supreme Court in *Davis v. Mississippi* held that taking fingerprints for identification purposes was permissible. [110] In *Davis* the fingerprints were excluded from evidence, not because they invaded any right of privacy, but because they were the product of an illegal detention.[111] The Court in *Davis* recognized that the fingerprinting process might, "under narrowly defined circumstances, be found to comply with the Fourth Amendment even though there is no probable cause in the traditional sense." [112] Federal courts have applied this reasoning to other means of identification, like handwriting and voice exemplars, with identical results. In *United States v. Dionisio* the Supreme Court, when accessing whether voice exemplars amounted to a search or seizure under the Fourth Amendment, compared them to face exemplars and concluded that a person has no reasonable expectation of privacy in either their face or voice. [113] Both are constantly exposed to the public. Because FaceIt does not involve any detention, the requirement of probable cause, or even the lesser standard of reasonable suspicion under *Terry v. Ohio*, federal law poses no barrier to American law enforcement's identical use of facial recognition technology.

Likewise, the Supreme Court held that a person may not have a reasonable expectation of privacy in their movements while in public. In *United States v. Knotts* the police were permitted to track a suspect's movement through the use of a "beeper." [114] The Court held that the Fourth Amendment was not implicated because visual surveillance of the defendant's movements from public places would have yielded the same information.

FaceIt's present ability to recognize people in public by their faces could conceivably be augmented by other abilities. Once passersby have been identified, it would be exceedingly easy to create a database of which individuals associated with each other. Additionally, Loronix Information Systems and TASC, Inc. have announced their partnership to develop behavioral recognition software. [115] Video cameras could be fed into a software program capable of identifying certain types of behavior or gestures. [116]

VII. The Harm of Mass Monitoring

Mass monitoring of the public, while possibly reducing crime in the areas where it is utilized, could have serious negative implications on our society. The enjoyment of privacy is not the only thing that would suffer. Widespread monitoring hinders discourse and spontaneity.

> Free discourse – a First Amendment value – may be frivolous or serious, humble or defiant, reactionary or revolutionary, profane or in good taste; but it is not free if there is surveillance. Free discourse liberates the spirit, though it may produce only froth. The individual must keep some facts concerning his thoughts within a small zone of people. At the same time he must be free to pour out his woes or inspirations or dreams to others. He remains the sole judge as to what must be said and what must remain unspoken. This is the essence of the idea of privacy implicit in the First and Fifth Amendments as well as in the Fourth. [117]

A key concept of social control theory is the authority of the observer over the observed, with the result that those subject to scrutiny are less likely to express themselves in ways that might distinguish them or draw attention. [118]

> Privacy is the basis of individuality. To be alone and be let alone, to be with chosen company, to say what you think, or don't think but to say what you will, is to be yourself. Solitude is imperative... [119]

Another concern is the effect on the right to free association. Social psychologists assert that video taping political events can affect the participant's self-image because of the association between surveillance and criminality. [120] The result is a discouragement at the

individual level to participate in political demonstrations. [121]

VIII. Conclusion

It is probably fair to say that the American public's expectations of privacy have been diminished since the *Katz* decision. At the very least, we are concerned. Ninety-two percent of respondents answered a Harris-Westin poll in 1997 saying that they were concerned about threats to privacy, the highest result since the poll began in the 1970s. [122]

Advancements in eavesdropping technology have the effect of lowering our expectations of privacy, which in turn makes it procedurally easier for the government to use the technology to observe its own citizens. Since current federal jurisprudence presents no impairment to the mass monitoring of the public, how is the American public to prevent such a thing from happening?

To some extent we can trust the institutions of government to set a policy against mass monitoring. When the state of Michigan converted to digitized photos, which could be stored in a database, a decision was made by the policy division of the Secretary of State's office not to incorporate facial recognition technology because of the privacy concerns implicated. [123] Likewise, an Orlando city commissioner led a movement in 1996 to do away the city's street surveillance system because privacy might suffer from a lack of restrictions on the system. [124]

Some members of the federal government have expressed their concerns about mass monitoring. U.S. House Majority Leader Dick Armey said in regards to FaceIt, "Do we really want a society where one cannot walk down the street without Big Brother tracking our every move?" [125] Armey called for congressional hearings on the subject and an investigation into the use of federal funds in the development of facial recognition technology. [126]

Rather than placing our trust in governmental entities to follow the same policy struck by Michigan and Orlando, the better course for insuring the privacy we enjoy in public places would be to raise our objections to mass monitoring through our respective legislatures. By doing so, the public would be declaring to the government what their expectations are with regard to privacy in public places. Such an approach would probably meet with less resistance from the

judicial system. When the dispute in *Olmstead* was before Justice Taft, he stated his reluctance to attribute "an enlarged and unusual meaning to the Fourth Amendment" and suggested that if a right to privacy in telephone conversations was to be recognized, then Congress was free to do so. [127]

Sixty years passed from the *Olmstead* decision to the passage of the Omnibus Crime Control and Safe Streets Act, which addressed telephone surveillance. Better late than never. Hopefully, the legislatures of this nation will address the issue of mass monitoring of public spaces in a more timely fashion.

---

[1] J.D. Candidate, University of Richmond, 2002; B.A. in Writing with English Honors, Millikin University, 1993. The author is an Articles Editor of the Richmond Journal of Law & Technology. He would like to thank Professor Ronald Bacigal and Professor Rodney Smolla for their support and invaluable comments.

[2] *See* GEORGE ORWELL, 1984, 4-8 (Harcourt Brace Jovanovich, Inc. 1977) (1949).

[3] United States v. Katz, 389 U.S. 347 (1967).

[4] Christopher S. Milligan, *Facial Recognition Technology, Video Surveillance, and Privacy*, 9 S. CAL. INTERDISC. L.J. 295, 313 (Winter 1999).

[5] *Id.* at 313-14 (Winter 1999).

[6] Griswold v. Connecticut, 381 U.S. 479 (1965).

[7] Roe v. Wade, 410 U.S. 113 (1973).

[8] Whalen v. Roe, 429 U.S. 589 (1977).

[9] Bowers v. Hardwick, 478 U.S. 186 (1986).

[10] *See* Milligan, *supra* note 3, at 313-14.

[11] U.S. CONST. amend. IV.

[12] United States v. Brignoni-Ponce, 422 U.S. 873, 878 (1975).

[13] Schmerber v. California, 384 U.S. 757, 767 (1966).

[14] Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 619 (1989).

[15] Olmstead v. United States, 277 U.S. 438, 464 (1928).

[16] Id. At 464-66.

[17] *Katz*, 389 U.S. at 353, 356.

[18] *Id*. at 351, 353.

[19] Rodney A. Smolla, *Privacy and the First Amendment Right to Gather News*, 67 GEO. WASH. L. REV. 1097, 1118 (1999).

[20] Oliver v. United States, 466 U.S. 170 (1984).

[21] California v. Greenwood, 486 U.S. 35 (1988).

[22] In United States v. Long, 176 F.3d 1304 (1999), the defendant kept his garbage in opaque garbage bags and placed then on top of his trailer to make them less accessible to the public. The court held the defendant's expectation of privacy was still unreasonable.

[23] *See* United States v. Place, 462 U.S. 696 (1983).

[24] *See* Jacobson v. United States., 503 U.S. 540 (1992) (See Comment)
[25] *See* Cardwell v. Lewis, 417 U.S. 583 (1974).

[26] *See* Smith v. Maryland, 442 U.S. 735, 743-744 (1979).

[27] *See* Florida v. Riley, 488 U.S. 445 (1989).

[28] *See* Dow Chemical Co. v. United States, 476 U.S. 227 (1986).

[29] Greg Miller, *Big Ear of the Law Tames Town's Gunfire: Redwood City's $100,000 System Uses Hidden Microphones, Computers to Pinpoint Gunshots*, L.A. TIMES, Jan. 12, 1998, at D3, *avaliable at* 1998 WL 2388046 and LEXIS, News Library. *See also* Marshall Wilson, *Redwood City Endorses Gunshot Locator System*, S.F. CHRON., Mar. 18, 1997, at A15, *available at* 1997 WL 6693664 *and* LEXIS, News Library.

[30] Greg Miller, *Big Ear of the Law Tames Town's Gunshots: Redwood City's $100,000 System Uses Hidden Microphones, Computers to Pinpoint Gunfire*, L.A. TIMES, Jan. 12, 1998, at D3, *available at* 1998 WL 2388046 and LEXIS, News Library.

[31] Brian Rooney, *New Technology to Track Gunfire*, World News Tonight (ABC News television broadcast, July 5, 2000), *available at* LEXIS, News Library.

[32] *Id.*

[33] *Id. See also* Paul Elias, *Shot Spotter Technology Sparks Concern*, *at*

http://www.techtv.com/cybercrime/features/story/0,23008,2101015,00.html (last visited Jan. 18, 2001).

[34] Paul Elias, *Shot Spotter Technology Sparks Concern*, *at* http://www.techtv.com/cybercrime/features/story/0,23008,2101015,00.html (last visited Jan. 18, 2001).

[35] *See* Paul Elias, *Shot Spotter Technology Sparks Concern*, *at* http://www.techtv.com/cybercrime/features/story/0,23008,2101015,00.html (last visited Jan. 18, 2001). *See also* Gary Fields, *"Spotter" Pinpoints a Shot in the Dark Microphones monitor area in L.A. County*, USA TODAY, June 16, 2000, at 3A, *available at* LEXIS, News Library; Lisa Benavides, *L.A. Police Buying Into Local Anti-crime Technology*, TENNESSEAN, Oct. 10, 1999, at 3E, *available at* LEXIS, News Library; Brian Rooney, *New Technology to Track Gunfire*, World News Tonight (ABC News television broadcast, July 5, 2000), *available at* LEXIS, News Library.

[36] *See* Lisa Benavides, *L.A. Police Buying Into Local Anti-crime Technology*, TENNESSEAN, Oct. 10, 1999, at 3E, *available at* LEXIS, News Library; Gary Fields, *"Spotter" Pinpoints a Shot in the Dark Microphones monitor area in L.A. County*, USA TODAY, June 16, 2000, at 3A, *available at* LEXIS, News Library; Paul Elias, *Shot Spotter Technology Sparks Concern, at* http://www.techtv.com/cybercrime/features/story/0,23008,2101015,00.html (last visited Jan. 18, 2001).

[37] Fred Wayne, *Police Get Computerized Hand in Gunshot Detection*, (CNN television broadcast, Dec. 25, 1995, transcript #58-5), *available at* LEXIS, News Library.

[38] Eve Mitchell, *New System for Finding the Location of Gunshots to be Tested*, PITTSBURGH POST-GAZETTE, July 21, 1996, at A6, (reprinted from S.F. EXAMINER), *available at* LEXIS, News Library.

[39] Press Release, Trilon Technology, Using Technology in the Fight Against Random Gunfire (Apr. 3, 2000) *available at* http://www.shotspotter.com/g-pr-apr00b.html (last visited Jan. 18, 2001).

[40] Lisa Benavides, *L.A. Police Buying Into Local Anti-crime Technology*, TENNESSEAN, Oct. 10, 1999, at 3E, *available at* LEXIS, News Library.

[41] *Id*.

[42] *Id.*

[43] *Id.*

[44] Tanya Bricking, *Detectors to Hear Gunshots Suggested*, CINCINNATI ENQUIRER, Mar. 24, 1999, at B2, *available at* 1999 WL 9428438 and LEXIS, News Library.

[45] *Id.*

[46] Gary Fields, *"Spotter" Pinpoints a Shot in the Dark Microphones monitor area in L.A. County*, USA TODAY, June 16, 2000, at 3A, *available at* LEXIS, News Library; Greg Miller, *Big Ear of the Law Tames Town's Gunfire: Redwood City's $100,000 System Uses Hidden Microphones, Computers to Pinpoint Gunfire*, L.A. TIMES, Jan. 12, 1998, at D3, *available at* 1998 WL 2388046 and LEXIS, News Library; Marshall Wilson, *Redwood City Endorses Gunshot Locator System*, S.F. CHRON., Mar. 18, 1997, at A15, *available at* 1997 WL 6693664 and LEXIS, News Library; Paul Elias, *Shot Spotter Technology Sparks Concern*, *at* http://www.techtv.com/cybercrime/features/story/0,23008,2101015,00.html (last visited Jan. 18, 2001).

[47] Gary Fields, *"Spotter" Pinpoints a Shot in the Dark Microphones monitor area in L.A. County*, USA TODAY, June 16, 2000, at 3A, *available at* LEXIS, News Library; Paul Elias, *Shot Spotter Technology Sparks Concern*, *at* http://www.techtv.com/cybercrime/features/story/0,23008,2101015,00.html (last visited Jan. 18, 2001).

[48] Gary Fields, *"Spotter" Pinpoints a Shot in the Dark Microphones monitor area in L.A. County*, USA TODAY, June 16, 2000, at 3A, *available at* LEXIS, News Library; Marshall Wilson, *Redwood City Endorses Gunshot Locator System*, S.F. CHRON., Mar. 18, 1997, at A15, *available at* 1997 WL 6693664 and LEXIS, News Library.

[49] Greg Miller, *Big Ear of the Law Tames Town's Gunfire: Redwood City's $100,000 System Uses Hidden Microphones, Computers to Pinpoint Gunshotsfire*, L.A. TIMES, Jan. 12, 1998, at D3, *available at* 1998 WL 2388046 and LEXIS, News Library.

[50] Greg Miller, *Big Ear of the Law Tames Town's Gunfire: Redwood City's $100,000 System Uses Hidden Microphones, Computers to Pinpoint Gunshots*, L.A. TIMES, Jan. 12, 1998, at D3, *avaliable at* 1998 WL 2388046 and LEXIS, News Library; Trilon Technology Home Page, *Frequently Asked Questions*, *available at* http://www.shotspotter.com/g-faq.html#01 (last visited Jan. 18, 2001).

[51] *Id*.

[52] Paul Elias, *Shot Spotter Technology Sparks Concern*, *at* http://www.techtv.com/cybercrime/features/story/0,23008,2101015,00.html (last visited Jan. 18, 2001).

[53] *Id*.

[54] Gary Fields, *"Spotter" Pinpoints a Shot in the Dark Microphones monitor area in L.A. County*, USA TODAY, June 16, 2000, at 3A, *available at* 2000 WL 5781347 and LEXIS, News Library.

[55] Tanya Bricking, *Detectors to Hear Gunshots Suggested*, CINCINNATI ENQUIRER, Mar. 24, 1999, at B2, *available at* 1999 WL 9428438 and LEXIS, News Library.

[56] *Id.*

[57] *See* Jonathan Zittrain, *A New Legal Paradigm? What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication*, 52 STAN. L. REV. 1201, 1215 (May 2000).

[58] *See* Greg Miller, *Big Ear of the Law Tames Town's Gunfire: Redwood City's $100,000 System Uses Hidden Microphones, Computers to Pinpoint Gunshots*, L.A. TIMES, Jan. 12, 1998, at D3, *avaliable at* 1998 WL 2388046 and LEXIS, News Library.

[59] Marshall Wilson, *Decision Due on Gunfire Locator: Novel Rooftop Sensors Face Critical Test in Redwood City*, S.F. CHRON., Mar. 17, 1997, at A16, *available at* 1997 WL 6693603 and LEXIS, News Library.

[60] Marshall Wilson, *Redwood City Endorses Gunshot Locator System*, S.F. CHRON., Mar. 18, 1997, at A15, *available at* 1997 WL 6693664 and LEXIS, News Library.

[61] *Id*.

[62] Gary Fields, *"Spotter" Pinpoints a Shot in the Dark Microphones monitor area in L.A. County*, USA TODAY, June 16, 2000, at 3A, *available at* 2000 WL 5781347 and LEXIS, News Library.

[63] *See* Marshall Wilson, *Decision Due on Gunfire Locator: Novel Rooftop Sensors Face Critical Test in Redwood City*, S.F. CHRON., Mar. 17, 1997, at A16, *available at* 1997 WL 6693603 and LEXIS, News Library.

[64] Trilon Technology Home Page, *Frequently Asked Questions*, *available at* http://www.shotspotter.com/g-faq.html#01 (last visited Jan. 18, 2001).

[65] Hoffa v. United States, 385 U.S. 293, 302 (1966).

[66] United States v. White, 401 U.S. 745 (1971) (holding that the government can monitor, record or transmit communications so long as one party to a private conversation consents.)

[67] United States v. Mankani, 738 F.2d 538, 542 (2d Cir. 1984).

[68] *Id*. at 541-43.

[69] United States v. Agapito, 620 F.2d 324, 329-332 (2d Cir. 1980)

[70] United States v. Llanes, 398 F.2d 880 (2d Cir. 1968)

[71] *Agapito,* 620 F.2d at 329-30.

[72] Mankani, 738 F.2d at 543.

[73] *Id*. at 544.

[74] 18 U.S.C. § 2510(2) (2001).

[75] United States v. Hagarty, 388 F.2d 713, 716 (7th Cir. 1968).

[76] *Agapito,* 620 F.2d at 330.

[77] Jennifer Mulhern Granholm, *Video Surveillance on Public Streets: The Constitutionality of Invisible Citizen Searches,* 64 U. DET. L. REV. 687, 687-88 (Summer 1987).

[78] Milligan, *supra* note 3, at 319.

[79] Quentin Burrows, *Scowl Because You're on Candid Camera: Privacy and Video Surveillance,* 31 VAL. U.L. REV. 1079, 1104 (Summer 1997).

[80] *See* Milligan, *supra* note 3, at 325 (citing Mark Boal, *Spycam City*, VILLAGE VOICE, Oct. 6, 1998, at 38, *available at* 1998 WL 20492919).

[81] Mark Boal, *Spycam City*, VILLAGE VOICE, Oct. 6, 1998, at 38, *available at* 1998 WL 20492919.

[82] William M. Bulkeley, *Your Face or Mine? Ask a Computer,* WALL ST. J. December 7, 1999, at 1, *available at* and LEXIS, Newspaper Library.

[83] *Id*.

[84] *Id.*

[85] *Id*.

[86] *Visionics to Unveil Third Generation FaceIt Engine; Announces Breakthrough in Facial Recognition Technology*, BUSINESS WIRE, May 7, 1999, *available at* LEXIS, News Library.

[87] Richard Saltus, *In Your Face Face-Recognition is Taking Off, but Some Fear "Big Brother" is Watching*, BOSTON GLOBE, Feb. 22, 2000, at E1, *available at* Lexis, News Library; *Government Awards London Borough With Major Grant to Expand CCTV Surveillance Program*, BUSINESS WIRE, Feb. 7, 2000, *available at* LEXIS, News Library.

[88] *Government Awards London Borough With Major Grant to Expand CCTV Surveillance Program*, BUSINESS WIRE, Feb. 7, 2000, *available at* LEXIS, News Library.

[89] *In Your Face Face-Recognition is Taking Off, but Some Fear "Big Brother" is Watching*, BOSTON GLOBE, Feb. 22, 2000, at E1, *available at* Lexis, News Library.

[90] Beth Fitzgerald, *Jersey City, N.J. Firm Offers Software to Recognize Criminals*, STAR-LEDGER, Feb. 16, 2000.

[91] Richard Saltus, *In Your Face Face-Recognition is Taking Off, but Some Fear "Big Brother" is Watching*, BOSTON GLOBE, Feb. 22, 2000, at E1, *available at* Lexis, News Library.

[92] *Government Awards London Borough With Major Grant to Expand CCTV Surveillance*

Program, BUSINESS WIRE, Feb. 7, 2000, *available at* LEXIS, News Library (citing up to a 70% reduction in crime); *Tony Blair Gets a First Hand Look at FaceIt Surveillance System At Newham: Major Crime Reduction in London Borough Sparks Visit From British Prime Minister*, BUSINESS WIRE, Feb. 15, 2000, *available at* LEXIS, News Library (citing a 40% reduction in crime); Beth Fitzgerald, *Jersey City, N.J. Firm Offers Software to Recognize Criminals*, STAR-LEDGER, Feb. 16, 2000.

[93] *Tony Blair Gets a First Hand Look at FaceIt Surveillance System At Newham: Major Crime Reduction in London Borough Sparks Visit from British Prime Minister*, BUSINESS WIRE, Feb. 15, 2000, *available at* LEXIS, News Library.

[94] Geoff Dutton, *Eye on Ybor*, TAMPA TRIBUNE, June 30, 2001, *available at* 2001 WL 5506205.

[95] Len Hindus, *Big Brother is Watching*, ADVANCED IMAGING, Apr. 1, 2001, at 30, *available at* 2001 WL 14103503.

[96] Luke Cyphers, *Keeping Eye on Super Fans*, N. Y. DAILY NEWS, Feb. 1, 2001, at 86, *available at* LEXIS, News Library. *See also* Dutton, *supra* note 96.

[97] *See* Hindus, *supra* note 97. *See also* Lee Cowan, *Face-Recognition Technology Used to Check Attendees at Super Bowl XXXV*, The Early Show (CBS News television broadcast, Feb. 2, 2001), *available at* LEXIS, News Library.

[98] *See* Dutton, *supra* note 93.

[99] *Id*.

[100] Vickie Chachere, *Tampa Uses New Face Scan Technology*, ASSOCIATED PRESS ONLINE, July 13, 2001, *available at* 2001 WL 24711985.

[101] *Id.*

[102] *See* Dutton, *supra* note 93.

[103] *See* Chachere, *supra* note 99.

[104] *See Id*.

[105] *See Id*.

[106] *See Id.*

[107] *See Identix/ANADAC Selected by the State of Maryland and Arlington County, Va. to Supply Advanced Photo Imaging and Identification System*, BUSINESS WIRE, Feb. 8, 1999, *available at* LEXIS, News Library.

[108] *See* Bulkeley, *supra* note 81.

[109] *See* Cyphers, *supra* note 95.

[110] Davis v. Mississippi, 394 U.S. 721, 727 (1969).

[111] *In re* Grand Jury Proceedings Mills, 686 F.2d 135, 137-38 (3d Cir. 1982).

[112] *Id.* at 137.

[113] United States v. Dionisio, 410 U.S. 1, 14 (1973).

[114] United States v. Knotts, 460 U.S. 276, 281 (1983). *See also* United States v Karo, 468 U.S. 705 (1984) (holding that the use of a motion tracking device only violated the defendant's Fourth Amendment rights when suspect entered his home, where he had a reasonable expectation of privacy, and the monitoring continued).

[115] PR NEWSWIRE *Loronix and Litton TASC Announce Partnership to Develop Next-Generation Video Surveillance System; Advanced New Technology Will Change the Face of Video Surveillance and Security in Retail and Other Markets* (Apr. 13, 2000), *available at* LEXIS, News Library.

[116] *Id*.

[117] United States v. White, 401 U.S. 745, 762-763 (1971).

[118] Milligan, *supra* note 3, at 327 (citing Mark Boal, *Spycam City*, VILLAGE VOICE, at 38, *available at* 1998 WL 20492919).

[119] *White*, 401 U.S. at 763.

[120] Milligan, *supra* note 3, at 328 (citing Mark Boal, *Spycam City*, VILLAGE VOICE, at 38, *available at* 1998 WL 20492919).

[121] *See Id*.

[122] Mark Boal, *Spycam City*, VILLAGE VOICE, Oct. 6, 1998, at 38, *available at* 1998 WL 20492919.

[123] *See* Bulkeley, *supra* note 81.

[124] Burrows, *supra* note 78, at 1079.

[125] *See Id.*

[126] *FaceIt Use Faces Scrutity*, ORLANDO SENTINEL, July 12, 2001, at D2, available at 2001 WL 9196479.

[127] Olmstead v. United States, 277 U.S. 438, 465-467 (1928).