7 Va. J.L. & Tech. 2 (2002), *at* http://www.vjolt.net

VIRGINIA JOURNAL *of* LAW *and* TECHNOLOGY

UNIVERSITY OF VIRGINIA	SPRING 2002	7 VA. J.L. & TECH. 2

Here's Looking At You, Kid: Has Face-Recognition Technology Completely Outflanked The Fourth Amendment?

By Alexander T. Nguyen*

---

* J.D. Candidate, Yale Law School, 2003. I would like to thank Anita Allen-Castellitto for her guidance throughout this project.

A man finds room in the few square inches of the face for the traits of all his ancestors, for the statement of all his history, and his wants.
—Ralph Waldo Emerson

The serial number of a human specimen is the face, that accidental and unrepeatable combination of features. It reflects neither character nor soul, nor what we call the self. The face is only the serial number of a specimen.
—Milan Kundera

I. INTRODUCTION: ARGUS-EYED TECHNOLOGY

1. In January 2001, roughly 100,000 ticket-holders who came to watch the Super Bowl in Tampa, Florida, were being watched themselves, not by people, but by cameras equipped with face recognition software. Unbeknownst to the spectators, these cameras scanned each individual face in the stadium and a computer matched their profiles against a central database of known criminals.[1] The Argus-eyed system identified nineteen individuals. However, since they were petty ticket scalpers and pickpockets,[2] the police did not bother to make any arrests.[3] Still, this face recognition technology has drawn big protests,[4] with civil rights advocates calling the technology "a computerized police lineup"[5] that raised serious questions about possible violations of the Fourth Amendment guarantee to be free from "unreasonable searches and seizures."[6] Company officials and law enforcement officials have argued that the technology makes neighborhoods safer (cameras are everywhere),[7] could eliminate racial profiling (cameras process *every* face),[8] raises no constitutional concerns (cameras scan public places only),[9] and can even enhance privacy in certain uses

[1] Barbara Dority, *A Brave New World—Or a Technological Nightmare? Big Brother is Watching!*, HUMANIST, May 1, 2001.
[2] *Id.*
[3] Jim Loney, *Super Bowl Surveillance Draws Protest From ACLU*, REUTERS, Feb. 2, 2001.
[4] Geoff Dutton, *Eye on Ybor*, TAMPA TRIBUNE, June 30, 2001, at 1.
[5] Howard Simon, Florida ACLU director, as quoted in Loney, *supra* note 3.
[6] "We fully understand that while everyone has a reduced expectation of privacy while in public, including sitting in the stands with one's family at a Sunday afternoon football game, we do not believe that the public understands or accepts that they will be subjected to a computerized police lineup as a condition of admission." Letter from Howard Simon and Michael Pheneger of the ACLU to Tampa Mayor Dick Greco (Feb. 1, 2001), *at* http://www.aclu.org/news/2001/n020101a.html.
[7] Visionics, creator of FaceIt notes on its website that crime has dropped 34% in Newham, England, where cameras with facial recognition software were installed. Similarly, crime has also dropped in casinos, European soccer matches and town centers where such cameras have been installed. *See* http://www.visionics.com.
[8] "Facial recognition systems, by contrast, do not focus on a person's skin color, hairstyle or manner of dress, and they do not recognize racial stereotypes. While there is a danger that the system may make an incorrect match, that danger is no more exaggerated than it is when traditional identification methods, such as comparing mug shots, are used." John Woodward Jr., *And Now, the Good Side of Facial Profiling*. THE WASHINGTON POST, Feb. 4, 2001, at B4.
[9] "The law states that there is no expectation of privacy by an individual on a public street." Bill Todd, *Give Police Best Tools to Fight Crime*, TAMPA TRIBUNE, July 28, 2001, at 17.

(cameras prevent identity theft).[10] The use of biometric technology is predicted to be one of the fastest-growing industry fields today.[11] Face-recognition systems have been hailed as an "emerging technology that will change the world."[12]

2. Rapid advancement in the field of sense-enhancing surveillance technology has been a Faustian bargain for a society concerned with protecting privacy and security at the same time. In the resulting trade-off over the past few decades, privacy has been eroded in the name of public safety. As the Fourth Amendment's "reasonable expectation of privacy standard" formulated in *Katz v. United States*[13] has become more and more difficult to apply, a jurisprudence has developed that would almost guarantee that cameras linked to facial recognition software such as FaceIt would pass constitutional muster. This is because there is neither a *subjective* expectation of privacy in a face (citizens do not mask themselves) nor is there an *objective* expectation of privacy (surveillance takes place in public). Yet the omnipresence—and the potential omniscience—of cameras that can identify and potentially track individuals is the most Orwellian scenario that we can imagine in a modern society. How might courts address the constitutionality of this problem? More importantly, how might privacy advocates reinvigorate the importance of privacy expectations even in the public square and oppose face-recognition technology constitutionally?

3. This article will argue that the "reasonable expectation of privacy" doctrine outlined in Katz has outlived its usefulness and is helpless against face recognition software in public, but that two alternatives exist. The first source of protection for citizens can be drawn from a reading of the Fourth Amendment that emphasizes *government accountability* as the basis for limitations on search and seizure—under this conception, searches are restricted not because they inconvenience citizens, but because government searches must be *justified* and *explained* to the individual citizen. The second source of protection can be drawn from the court's historical protection of anonymity. This article will argue that anonymity—traditionally protected as part of speech and the First Amendment—has been applied especially in public and hence might offer constitutional protection against face recognition technology. Together, the two might be able to offer constitutional shields that citizens can use against the omnipresent eye of the government.

4. This article is divided into six parts. Part I briefly describes the technology of biometrics—identification technology based on the dimensions of an individual's physical characteristics—and how facial recognition software promises to be the most powerful advancement yet because of its non-intrusiveness and close link with the computer. Part II briefly traces the Court's jurisprudence in the Fourth Amendment as it pertains to technologically-assisted physical surveillance. Part III derives some general principles to be

---

[10] Lisa Bowman, *Firm Defends 'Snooper Bowl' Technology*, CNET NEWS, Mar. 9, 2001, *at* http://news.cnet.com/news/0-1005-200-5079810.html.

[11] The McLean Group, Making a Market in Biometrics, Presentation to the IBIA (Sept. 15, 1999), *available at* http://www.ibia.org/mcleangroup.PDF (quoting a *Lehman Brothers 1999 Security Industry Overview*, from Mar. 30, 1999: "Although the biometric device industry may be less than $100 million today, we estimate that this market will grow 30%-35% annually to reach $400 million in five years.").

[12] *10 Emerging Technologies that Will Change the World*, MIT TECHNOLOGY REVIEW, Jan. 1, 2001.

[13] 389 U.S. 347 (1967).

drawn from this jurisprudence and argues that under the current standard, technology such as FaceIt is almost certain to pass constitutional muster. Part IV argues that ironically this technology that has the greatest Orwellian and intrusive potential at the same time would clear the bar for constitutionality, and that constitutional protection is needed against such technologies as FaceIt. Part V suggests that one source of such constitutional protection is a re-reading of the Fourth Amendment as requiring government accountability—under this standard, government searches have to be announced and explained, and the searching of innocent citizens might not be allowed. Part VI suggests another, more immediately available, source of constitutional protection in anonymity. It will be argued in that section that anonymity has traditionally been protected by the Court as part of speech, but that there is some evidence that the two can be decoupled such that anonymity can be considered a *per se* right, and thus offer the protection against technology such as FaceIt.

II. THE BIOMETRIC FRONTIER: FROM THUMBPINTS TO FACE-BASED SURVEILLANCE

A. A (VERY) BRIEF HISTORY OF BIOMETRICS

5. Biometrics uses the body as a password. It relies on the dimensions of a person's physical characteristics for identification.[14] Such physical characteristics might include fingerprints, voices, iris, retinas, blood, and other traits.[15] The use of biometrics in law enforcement dates back to the 19th Century, when Parisian anthropologist Alphonse Bertillion created the first biometric database of criminals who used various aliases and hence made alphabetically cataloguing repeat offenders futile.[16] Bertillion indexed biometric dimensions such as a suspect's circumference of the head or the length of the middle finger and filed them according to their *size*. The system proved highly effective and over the next decade; 120,000 criminals had been indexed in Paris. By the beginning of the 20th Century, 20 prisons and seven police stations in America had adopted Bertillion's system.[17] As prisons became more bureaucratic, and files were kept, some prisons included on the files a single space for "description"—this space was used to record biometric information to identify repeat offenders.[18]

6. Fingerprinting (alluded to in Mark Twain's *Pudd'nhead Wilson*[19], for example) was another important biometric. Fingerprints are unique to each individual, including even identical twins since they result from genes as well as random processes during pregnancy.[20] Fingerprinting was an important development, because its use is specific to crime fighting. In America, there has not been a mandatory program under which citizens have to give the government their fingerprints; only criminals are made to give them.[21] However, it is to be noted that certain classes of citizens have always been fingerprinted for a variety of

---

[14] John Woodward, Jr., *Super Bowl Surveillance: Facing up to Biometrics,* 2001 RAND ARROYO CTR. 3, *available at* http://www.rand.org/publications/IP/IP209/IP209.pdf (last visited Apr. 15, 2002).
[15] *Id*
[16] SIMON GARFINKEL, DATABASE NATION: THE DEATH OF PRIVACY IN THE 21st CENTURY (2000) 40.
[17] *Id.* at 40.
[18] SIMON COLE, A HISTORY OF FINGERPRINTING AND CRIMINAL IDENTIFICATION 11 (2001). At the Pennsylvania Penitentiary in Philadelphia, for example, clerks used words such as "sallow" or "fresh" to describe inmates.
[19] MARK TWAIN, PUDD'NHEAD WILSON 62 (Edited by Malcolm Bradbury, Penguin Classics, 1986) (1894).
[20] GARFINKEL, *supra* note 16, at 45.
[21] *Id*.

purposes. These citizens include welfare recipients,[22] customers who want to cash a check,[23] drivers,[24] immigrants,[25] and others.[26] Secondly, and more importantly, fingerprints opened the door for the computer. As the fingerprinting databases grew, they became inefficient—it took staffers a longer time to sift through piles of index cards to match the prints. These databases would have collapsed under their own weight had computers not come to the rescue. Thus, in 1985, a Los Angeles detective trying to identify a single fingerprint would have had to look through 1.7 million fingerprint cards—a task that would have taken one technician 67 years. But today, a computer can do it in five minutes.[27] Known as the Automatic Fingerprint Identification System (AFIS), a computer reduced an entire fingerprint to a set of coordinates and was able to match fingerprints very quickly and very accurately.[28]

B. THE MOST OBVIOUS BIOMETRIC OF ALL: FACES AND FACEIT

7. FaceIt works on the same principle as AFIS—it reduces the facial features to a set of numbers (the width of the nose or the location of the temples, for example) and then matches them up against a database.[29] The development of this technology was spurred by significant government funding by entities such as the Office of Naval Research and the Defense Advanced Research Projects Agency (DARPA) in the late 1980s and early 1990s.[30] Essentially, FaceIt is a facial recognition software engine helping a network of cameras and computers to quickly detect and recognize faces.[31] When a head-like object moves within the camera's field of vision—both eyes have to be visible and the face cannot be turned

---

[22] Hugo Martin, *County Welfare Recipients Fingerprinted Social Services: Computer Finds Only Two Cases of Fraud But 700 People Have Refused to Participate in Controversial Program*, L.A. TIMES, Oct. 12, 1991, at B1.
[23] Juan Espinosa, *Businesses May Require Fingerprint to Cash Checks*, KNIGHT-RIDDER TRIBUNE BUSINESS NEWS, Dec. 7, 2001.
[24] Kimberly Kindy, *Failure to Fingerfraud Crime: DMV's Thumbprint Database is Insufficient—and Costly to Fix,* ORANGE COUNTY REGISTER, Dec. 31, 2000.
[25] Dina Elboghdady & Guillermo X. Garcia, *INS Streamlines Fingerprinting*, ORANGE COUNTY REGISTER, Nov. 15, 1997.
[26] *See*, *e.g.*, Robert Trigaux, *They Want Your Prints*, ST. PETERSBURG TIMES, Feb. 23, 1997, at 1H. The detailed history of fingerprinting is outside the scope of this article, but see for more information, COLIN BEAVAN, FINGERPRINTS: THE ORIGINS OF CRIME DETECTION AND THE MURDER CASE THAT LAUNCHED FORENSIC SCIENCE (2001).
[27] David Johnston, *Computer Could Point Finger at Murderers: Automated Searches Through Fingerprint Files could Substantially Increase Arrests in L.A.*, L.A. Times, June 28, 1985.
[28] GARFINKEL, *supra* note 16, at 45.
[29] Jeffrey Rosen, *A Cautionary Tale for a New Age of Surveillance*, N.Y. TIMES, Oct. 7, 2001, *at* http://www.nytimes.com/2001/10/07/magazine/07SURVEILLANCE.html.
[30] *Computerized Facial Recognition: A Technology with Broad Range of Real-World Applications*. Testimony of Joseph Atick, President and Chief ExecutiveOfficer of Visionics Corporation, *before the U.S. House of Representatives Comm. on Banking and Fin. Servs.* (1998), at http://www.house.gov/financialservices/52098dja.htm ("Thanks to funding of basic research by several agencies including the Office of Naval Research, the INS, and DARPA—the U.S. scientific community made some significant breakthroughs in understanding how the human brain performs facial recognition. Subsequently, these basic discoveries became the foundation for the commercial development of computerized facial recognition systems such as FaceIt technology.").
[31] Visionics Corp. *What is FaceIt?* (2001) at http://www.visionics.com. FaceIt is created by Visionics Corporation in Minnesota. It is a leading provider of Identification information systems that employ "biometric" technology, which is the science of identifying individuals by measuring distinguishing biological characteristics.

more than 45 degrees from the camera[32]—the computer guesses whether it is a face.[33] If the answer is yes, FaceIt crops the face from the background and 'normalizes' the image by compensating for size and lighting. The image is then subjected to a Local Feature Analysis that essentially generates a faceprint—a digital code encapsulating the measurements of the landmarks of a face and how they correlate.[34] The software compresses this print down to a very small file of 84 bytes. Accessories such as wigs, moustaches, glasses, even basic plastic surgery, will not affect identification.[35] Although company officials say that only fourteen features are needed to establish identity, FaceIt tracks 80 features—this redundancy allows for more accurate identification.[36]

8. Uses for facial recognition vary, both for privacy-diminishing and privacy-enhancing uses. FaceIt can be used for verification, or one-on-one matching.[37] This mode could potentially enhance privacy. For example, a faceprint is part of an ATM card, and FaceIt simply matches the live face print to the ATM card—the face acts as passcode.[38] A faceprint can be used either as a logon device (perimeter defense mechanism) or as continuous monitoring (continuous authentication).[39] This mode could enhance privacy as it bars others from identity theft. However, the most important and prominent use of FaceIt, especially in light of the increased security concerns brought about by terrorism,[40] is use for identification, or one-to-many searching.[41] In this mode, cameras sweep their field of visions for every face present and then FaceIt compares each face it scans in a crowd to those in a database of facial images, returning a list of matches with associated confidence levels.[42] The system can match over a million faces per second.[43] This is the type of use that was employed at the Tampa Superbowl, and it is this type of use that this article will primarily focus on because it carries with it the largest privacy implications, and because this use can easily be reconfigured to monitor, or to follow, the presence and position of certain individuals.[44] The wide use of this technology is being seriously considered by a range of police departments, municipal governments and federal authorities.[45]

---

[32] *Id*.
[33] *Id.*
[34] *Id.*
[35] *Id.*
[36] Joseph Atick, as quoted in *How the Facial Recognition Security System Works* (2001), *at* http://www.cnn.com/2001/COMMUNITY/10/01/atick/.
[37] http://www.visionics.com.
[38] The first such ATM was introduced in Texas in May 1999. Alexandra Stikeman, *Biometrics*, TECHNOLOGY REVIEW, *at* http://www.technologyreview.com/magazine/jan01/tr10_atick.asp.
[39] See http://www.visionics.com ("The first is perimeter defense mechanism; an authorized individual gains entry to a network or session after a one-time logon process. Thereafter, the system usually does not offer any authentication. With FaceIt, users can be continuously authenticated ensuring that at all times, the individual in front of the computer or hand-held device continues to be the same authorized person who logged on."
[40] *See*, *e.g.,* Vickie Chachere, *Airport in Florida to Try Face Scanning*, ASSOCIATED PRESS, Dec. 14, 2001.
[41] http://www.visionics.com.
[42] *Id.*
[43] Ben Feller, *Lawmakers Hold off on FaceIt System*, TAMPA TRIBUNE, Dec. 14, 2001, at 8.
[44] http://www.visionics.com.
[45] *See*, *e.g.*, Sheila Cherry, *Big Brother Greets Visionics*, INSIGHT MAGAZINE, Oct. 22, 2001, at 22.

III. TECHNOLOGICALLY-ASSISTED PHYSICAL SURVEILLANCE AND THE FOURTH AMENDMENT

9. What does the Constitution have to say about all of this? To the dismay of privacy advocates, on first impression, it seems that even the wide spread use of FaceIt—this most Orwellian of technologies—would easily pass constitutional muster. All FaceIt does, after all, is simply look at faces—the most prominent part of the body that citizens expose to the public on the public street. And yet, the ubiquity of cameras capable of identifying every individual passing through the camera lenses' field of vision is the most dystopian that we can imagine. We are uneasy at having police officers using technology so powerful that it approaches Big Brother's omnipresence and omniscience. On the one hand, FaceIt is no different from a police officer standing at the corner with a set of mugshots and scanning for faces in the crowd.[46] On the other hand, however, FaceIt is, because of its accuracy and omnipresence, like having thousands of police officers standing in the square and monitoring citizens as they walk past to buy their groceries or enter restaurants. Viscerally, we are uncomfortable with that because in a totalitarian society, everything is public. Concentration camps and prisons undermine the dignity of inmates by stripping them of their privacy. Primo Levi wrote of Auschwitz, a Nazi concentration camp, that, "solitude in a Camp is more precious and rare than bread."[47] This is not to imply, of course, that FaceIt technology has the same pernicious effects as that of a concentration camp. It is, however, to underscore that the destruction of privacy has traditionally been a mark of societies that have placed little value on the ideals of freedom and liberty.

10. The Fourth Amendment—traditionally a shield against unwarranted government intrusion—seems useless in this context. It seems that technology has, this time, finally outflanked the Fourth Amendment, and that the sword of the Fourth Amendment has been dulled by dozens of technological advances that have preceded FaceIt. Is there any blood left within the stone of the Fourth Amendment to protect citizens from the arrival of this technology? Tracing the relevant line of cases that has brought us to this point might be useful. A look at history might offer a glimpse into destiny.

A. TECHNOLOGICALLY ENHANCED SENSES: EARS

11. 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."[48] In the traditional jurisprudence, Fourth Amendment violations were only found as a result of physical trespass. Even as wiretapping technology developed—technological innovations that enhanced ears—the Court strained to keep this requirement. In *Olmstead v. United*

---

[46] "Newcomb compares this use of facial recognition to a police officer standing on a corner with a mug book, comparing pictures with the faces of pedestrians, which is just an extension of patrol officers on the streets identifying suspects." K.C. Newcomb, Tampa police major responsible for implementing cameras at the Tampa Super Bowl. Michael Gips, *Face Off over Facial Recognition*, SECURITY MANAGEMENT, May 1, 2001.

[47] CHARLES SYKES, THE END OF PRIVACY 19 (1999), *citing* PRIMO LEVI, IF THIS IS A MAN: REMEMBERING AUSCHWITZ 329 (1985).

[48] The complete 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." U.S.C.A. CONST. AMEND. IV.

States[49] the Supreme Court held that tapping the phones of a bootlegger was neither a search nor a seizure. The taps were placed by inserting small wires along the defendants' telephone wires without any actual physical trespass on the property of the defendants.[50] The Court stated, "the evidence was secured by the use of the sense of hearing and that only."[51] In contrast, the Court ruled in *Silverman v. United States*[52] that the use of a spike-mike was an unconstitutional search since operation of the microphone required that it make actual physical contact with the heating duct of defendant's house—a procedure that was converted defendants' "entire heating system into a conductor of sound."[53] In ruling the conversations of illegal gambling inadmissible, the Court based its decision on "an unauthorized physical penetration into the premises occupied by the petitioners"[54], in essence applying the *Olmstead* holding. Already it was becoming more and more clear that the physical trespass requirement was beginning to matter less and less—the information obtained in *Olmstead* and that in *Silverman* were substantively not that much different, and to rule on the admissibility of evidence based on whether or not a device technically physically touched a heating duct and thus intruded was becoming slightly inane. The *Silverman* court here acknowledged the tension brought on by technology that eventually would bypass the physical trespass requirement, but then dismissed it as an issue to be addressed on another day.[55]

12. That day came with the watershed case of *Katz v. United States*.[56] In *Katz*, a defendant bookie placed an incriminating phone call from inside a public phone booth. Law enforcement officials from the Federal Bureau of Investigation had attached an electronic listening and recording device "to the outside of the public telephone booth."[57] In ruling the conversation inadmissible, the Court first dispensed with the trespass requirement formulated in Olmstead, noting that the Fourth Amendment protected people and not places.[58] "The fact that the electronic device employed to achieve [the recording] did not happen to penetrate the wall of the booth can have no constitutional significance."[59] To base constitutional rights on such a technicality, the Court argued, was "bad physics as well as

---

[49] 277 U.S. 438 (1928).
[50] *Id.* at 457.
[51] *Id.* at 464. Similar decisions include Goldman v. United States, 316 U.S. 129 (1942) (holding that physically placing a detectaphone against an office wall to eavesdrop on conversations in adjoining office did not constitute trespass and hence was not a Fourth Amendment violation).
[52] 365 U.S. 505 (1961).
[53] *Id.* at 506.
[54] *Id.* at 509.
[55] *Id.* at 508-509 ("We are told that re-examination of the rationale of […] Olmstead v. United States […] is now essential in the light of recent and projected developments in the science of electronics. We are favoured with a description of 'a device known as the parabolic microphone which can pick up a conversation three hundred yards away.' We are told of a 'still experimental technique whereby a room is flooded with a certain type of sonic wave,' which, when perfected, 'will make it possible to overhear everything said in a room without ever entering it or even going near it.' We are informed of an instrument 'which can pick up a conversation through an open office window on the opposite side of a busy street.' The facts of the present case, however, do not require us to consider the large questions which have been argued. We need not here contemplate the Fourth Amendment implications of these and other frightening paraphernalia which the vaunted marvels of an electronic age may visit upon human society.").
[56] 389 U.S. 347 (1967).
[57] *Id.* at 348.
[58] *Id.* at 353.
[59] *Id.* at 353.

bad law."[60] In *Katz*, Justice Harlan formulated a test in his concurrence that has since become the prevailing standard in deciding Fourth Amendment cases. In essence, the two-pronged test requires the presence of a subjective expectation of privacy that society deems objectively reasonable.[61]

B. TECHNOLOGICALLY ENHANCED SENSES: EYES

13. This standard—the expectation of privacy test—has come under much criticism, but the Court steadfastly applied it over the next decades. If the *Olmstead* line of cases dealt with electronically enhanced ears, this next line of cases, the most prominent of which are *California v. Ciraolo*[62] and *Dow Chemical Co. v. United States*[63] (both decided on the same day), dealt with enhanced eyes. In *Ciraolo*, the eyes of law enforcement were *not* technically enhanced. Defendant grower of marijuana used a 10-foot fence to shield his backyard—thereby showing his subjective expectation of privacy.[64] Law enforcement officers, however, used a private plane to fly over defendant's house at an altitude of 1,000 feet and photographed the backyard with a standard 35mm camera.[65] The Court argued that defendant's Fourth Amendment rights had not been violated because the marijuana was visible with "naked-eye observation"[66] from public airspace—hence there was no objective expectation of privacy. The Fourth Amendment, the *Ciraolo* court argued, does not require law enforcement officers "to shield their eyes when passing by a home on public thoroughfares."[67] The Court has similarly held that helicopter surveillance at 400 feet was not a Fourth Amendment violation.[68]

14. The same day as the *Ciraolo* decision, the Court ruled in *Dow Chemical*, that surveillance aided by technologically enhanced eyes did not violate the Fourth Amendment either. Here EPA officials boarded an airplane with a precision aerial camera after having been denied access for an on-site inspection, and instead took photographs of a chemical company's outdoor industrial complex. In permitting the photographs, the Court held that, "the mere fact that human vision is enhanced somewhat, at least to the degree here, does not give rise to constitutional problems."[69] Besides, the Court noted, the technology used in this instance was commonly available.[70]

---

[60] *Id.* at 362 (Harlan, J., concurring).
[61] *Id.* at 361.
[62] California v. Ciraolo, 476 U.S. 207 (1986).
[63] Dow Chemical Co. v. U.S., 476 U.S. 227 (1986).
[64] 476 U.S. at 211 ("Clearly—and understandably—respondent has met the test of manifesting his own subjective intent and desire to maintain privacy as to his unlawful agricultural pursuits.").
[65] *Id.* at 209.
[66] *Id.* at 213.
[67] *Id.* at 213.
[68] 488 U.S. 445 (1989).
[69] 476 U.S. at 238 ("It may well be […] that surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public, such as satellite technology, might be constitutionally proscribed absent a warrant. But the photographs here are not so revealing of intimate details as to raise constitutional concerns. Although they undoubtedly give EPA more detailed information than naked-eye views, they remain limited to an outline of the facility's buildings and equipment.").
[70] *Id.* at 231 ("The photographs at issue in this case are essentially like those commonly used in mapmaking.").

C. TECHNOLOGICALLY ENHANCED SENSES: LEGS

15. The expectation of privacy test also extended to the use of beepers to track and follow suspects—in this sense, they can be thought of as technologically enhanced legs. In *United States v. Knotts*[71] a beeper was placed into a chloroform container and sold to defendants suspected of manufacturing illegal substances. By monitoring the signal the beeper emitted, police followed defendants to their cabin. The court noted that the technology used in this instance "amounted principally to the following of an automobile on public streets and highways" where there is no expectation of privacy.[72] "Nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case."[73] On the other hand, the monitoring of a beeper inside a private residence, "a location not open to visual surveillance" was found to violate the Fourth Amendment in *United States v. Karo*.[74]

16. This reasoning was extended even further in *Kyllo v. United States*.[75] Using thermal imaging technology to determine whether or not defendant was growing marijuana using hot lamps, the Supreme Court noted that such use constituted a Fourth Amendment violation. "Where, as here, the Government uses a [sense-enhancing] device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[76] Here the Court inched back towards a spatially-defined interpretation of the Fourth Amendment, declaring that, at the least, the Fourth Amendment protected the home. It could as easily have ruled thermal imaging constitutional as a search of heat that leaves the house—in this sense it would not be unlike a search of garbage that the Court has already held constitutional.[77] However, the Court ignored this analogy, and this is telling because it suggests that perhaps the Court felt uneasy at opening the door to sophisticated future technological surveillance.[78]

IV. APPLYING THE GUIDELINES FROM THE PAST TO FACEIT: A MOOT AFFAIR?

1. Technological enhancement and surveillance has left a gap. In *Katz*, the court dispensed with the physical intrusion requirement and held that the Fourth Amendment protected people, not places. But over the next several decades, as technological advances increased, the Court was increasingly uneasy about simply allowing technology to be used in an unbridled manner. It allowed enhanced ears and enhanced legs and enhanced eyes, but soon retreated back towards a space-specific interpretation of the Fourth Amendment as technology strode on and made surveillance inside the house possible. In the process, it has left any reasonable expectation of privacy in a public place completely eviscerated. It is in this context into

---

[71] 460 U.S. 276 (1983).
[72] *Id.* at 281-282 ("When [defendant] travelled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was travelling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property.")
[73] *Id.* at 282.
[74] 468 U.S. 705 (1984).
[75] 533 U.S. 27 (2001).
[76] 121 S.Ct. 2038, 2046 (2001).
[77] California v. Greenwood, 486 U.S. 35 (1988).
[78] *Leading Case,* 115 HARV. L. REV. 346 (2001).

which FaceIt enters. This section will argue that, as far as facial recognition technology is concerned, the technology is almost certain to pass constitutional muster. This is because the nature of the technology (its availability), the locus of the search (public), and the scope of the search (binary) all favor its constitutionality.

A. THE NATURE OF THE NEW TECHNOLOGY: NO BIG HURDLE.

1. The "general public use" requirement

2. The Supreme Court has held that one of the factors to be used in determining whether technologically enhanced searches violate the Fourth Amendment is whether the technology is available to the general public. The Court used this rationale in part to admit evidence in *Dow Chemical* and to exclude it in *Kyllo*. In *Dow Chemical*, the Court noted that if law enforcement were to use "highly sophisticated surveillance equipment not generally available to the public," its use might require a warrant.[79] However, public use does not mean that its presence is widespread—simply that it is available in the marketplace. After all, the camera used in *Dow Chemical* cost $22,000 and was advertised as the "finest precision aerial camera available."[80] Worse, this requirement that technology be publicly available to pass Fourth Amendment muster places citizens at the mercy of the marketplace and the descending costs of technology.

> Once a technology becomes widely available, its use is no longer proscribed because an individual's expectation of privacy against that method of surveillance is no longer accepted by society. However, this theory seems to create a descending Orwellian spiral in which the privacy of the home would 'hinge upon the outcome of a technological race of measure/counter-measure between the average citizen and the government—a race that the people will surely lose.'[81]

17. FaceIt technology has been widely advertised to various clientele, including government, private corporations, banks, and office buildings.[82] FaceIt technology is also "inexpensive"[83] and is compatible with "any standard off the shelf hardware."[84] Technology as user-friendly

---

[79] 476 U.S. at 238.

[80] T. Wade McKnight, *Passive, Sensory-Enhanced Searches: Shifting the Fourth Amendment "Reasonableness" Burden,* 59 LA. L. REV. 1243, 1260 (1999).

[81] *Id*. at 1260, citing United States v. Cusumano, 67 F.3d 1497 (10th Cir. 1995).

[82] Joseph Atick, CEO of Visionics, the company responsible for creating FaceIt has stated that interest in this software has always been present, but that since the terrorist attacks on September 11, 2001, demand has increased even more drastically. "Since [September 11], there has been a dramatic increase in interest, coming from airports and other organizations concerned with safety, public transportation, government buildings, stadiums, etc. At this point, I can't say what orders have come through and where they're going. We've had to put some of the international orders on a delayed schedule to accommodate the United States." Atick, as quoted in *How the Facial Recognition Security System Works*. CNN COMMUNITY, Oct. 1, 2001, *at* http://www.cnn.com/2001/COMMUNITY/10/01/atick/.

[83] *See supra* note 30, testimony of Joseph Atick before the U.S. House of Representatives Comm. on Banking and Fin. Servs. *Computerized Facial Recognition: A technology with broad range of real-world applications* (May 20, 1998).

[84] The FaceIt package also runs off Windows 95/98/NT/2000, for example. *See* http://www.visionics.com/. *See also* testimony of Joseph Atick before the U.S. House of Representatives Comm. on Banking and Fin. Servs. *Computerized Facial Recognition: A technology with broad range of real-world applications* (May 20, 1998).

and as easily available to the general public, corporations, and businesses as FaceIt is likely to tilt this factor in favor of constitutionality under current jurisprudence.

2. Enhancing or replacing senses?

18. In general, Courts have ruled that technology that simply *enhances* senses that police officers were born with do not raise Fourth Amendment issues while technology that *replaces* those senses may.[85] Thus, using technology that enhances what the eyes would see anyway is constitutional generally. Similarly, the high precision camera used in the fly-over in *Dow Chemical* or the flashlight used in *Texas v. Brown* to search the interior of a car at night also do not violate the Fourth Amendment.[86] There is no search with sensory-enhancing devices such as "artificial light, binoculars, and telescopes."[87] On the other hand, as the Court ruled in *Kyllo*, using thermal imaging devices to see what is going on within a house is not protected (since natural eyes could not see through walls).

19. To be sure, this dichotomy, while useful as a rule of thumb, is not without its difficulties: Is a dog-sniff a "technology" that enhances or replaces senses? On the one hand, dogs detect what human noses would otherwise miss, but the image of cops—in the absence of narcotics dogs—themselves sniffing luggage at airports is a ludicrous image. It is difficult to classify which senses FaceIt technology enhances or replaces. It is analogous to a cop standing at the street corner, and going through a book of mugshots, but on the other hand, FaceIt does far more: It scans *everyone* on the street and compares them to the book of mugshots—something that police officers do not do.

20. In addition, there is the problem of scale. From the cases above, it is clear that the Supreme Court has in general held that technology that simply enhances rather than replaces natural senses raise no Fourth Amendment concerns. However, on numerous occasions the court has implied that the *ubiquitous* use of such technology might raise constitutional problems. Thus, even as the *Knotts* court allowed police technology that were simply "augmenting the sensory faculties bestowed […] at birth"[88], it later stated that the perennial and ubiquitous use of such technology would imply constitutional concerns while reserving those issues for another day.[89] Despite these concerns, FaceIt is almost certain to pass constitutional muster.

B. THE LOCUS OF THE SEARCH: NO EXPECTATION OF PRIVACY IN PUBLIC

21. FaceIt is almost certain to pass constitutional muster because there is neither a subjective nor an objective expectation of privacy in public spaces. Unless an individual wears a veil or a mask every time he or she leaves an apartment, there is no subjective expectation of privacy. Courts have held that there is no expectation of privacy in what an individual knowingly

---

[85] Christopher Slobogin, *Technologically-Assisted Physical Surveillance: The American Bar Association's Tentative Draft Standards*. 10 HARV. J. LAW & TEC. 383 (1997).
[86] "The use of artificial means to illuminate a darkened area simply does not constitute a search, and thus triggers no Fourth Amendment protection." 460 U.S. 730, 740 (1983).
[87] Alyson Rosenberg, *Passive Millimeter Wave Imaging: A New Weapon in the Fight Against Crime or a Fourth Amendment Violation?*, 9 ALB. L.J. SCI. & TECH. 135, 144 (1998).
[88] 460 U.S. at 282.
[89] "[I]f such dragnet type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable." *Id.* at 284.

exposes to the public.[90] There is no part of the body, no feature of an individual, that, in America at least, is exposed as openly or often, and so a subjective expectation of privacy is certainly not present in the face. In *United States v. Dionisio*, a grand jury subpoenaed about twenty individuals seeking to obtain a voice sample in order to compare them with a recorded conversation that was in evidence. In ruling such a subpoena constitutional, the Court noted that:

> The physical characteristics of a person's voice, its tone and manner, as opposed to the content of a specific conversation, are constantly exposed to the public. Like a man's *facial characteristics*, or handwriting, his voice is repeatedly produced for others to hear. No person can have a reasonable expectation that others will not know the sound of his voice, *any more than he can reasonably expect that his face will be a mystery to the world*.[91]

Indeed, the taking of biometric measurements is often permitted by courts. In *Dionisio*, the Supreme Court explained that such seizure might only be prohibited by the Fourth Amendment if they were obtained as a result of unlawful detention of a suspect (for the taking of fingerprints),[92] or when an intrusion into the body is taken without a warrant (for the taking of a blood sample).[93] A voice sample, the court held in *Dionisio*, is considered "immeasurably further removed" from these examples.[94] In FaceIt technology, neither concern is relevant—a faceprint can be obtained without unlawful detention or any intrusion into the body whatsoever. If the *Dionisio* court proposed that a voice sample did not approach the taking of a fingerprint or blood sample, a face print is even further removed from potential constitutional protection. In taking a voice sample, the subject from whom the sample will be taken will have to be subjected to the small inconveniences of being asked to speak into a recorder. With FaceIt technology, even such *de minimis* imposition is lacking. Officers do not have to walk up to individuals and stop them, even for a pat-down.[95] In fact, the technology is employed in the most public spaces available and subjects do not even know that they are being sampled. The objective expectation of privacy is also lacking, not only because surveillance takes place in public, but because additionally, law enforcement officials could simply shift the objective prong of the test by lowering the expectation of privacy by announcing their technology in advance and then using it ubiquitously.[96] There is some circularity in the objective prong of the expectation of privacy standard, as many have pointed out: "If the government is bound only to respect people's expectations, it is not bound at all, for it can easily condition the citizenry to expect little or no privacy."[97] In any

---

[90] 389 U.S. at 351.
[91] 410 U.S. 1, 14 (1973) (emphasis added).
[92] Davis v. Mississippi, 394 U.S. 721 (1969).
[93] Schmerber v. California, 384 U.S. 757 (1966).
[94] United States v. Dionisio, 410 U.S. at 14.
[95] Terry v. Ohio, 392 U.S. 1 (1968).
[96] In fact, officials of companies that have manufactured face-recognition software have suggested this very approach. "[Peter Mazzaroni, chairman of the ASIS Privacy and Personnel Information Management Council] says the public outcry [at the Tampa Super Bowl] was so great presumably because fans weren't informed in advance. As with many CCTV [closed circuit TV] applications, he says, notifying the public or employees beforehand often makes objections disappear." Michael A. Gips, *News and Trends: Face Off Over Facial Recognition*, May, 2001, *available at* http://www.securitymanagement.com/library/001037.html.
[97] William Stuntz, *The Distribution of Fourth Amendment Privacy*, 67 GEO. WASH. L. REV. 1265, 1268 (1999).

case, using traditional Fourth Amendment jurisprudence as a guide, FaceIt would therefore most likely pass the constitutional inquiry.

C. YES OR NO? THE BINARY SCOPE OF THE SEARCH.

22. *Dionisio* is important on another ground, because it suggests that a court look to the subject matter of the search to determine whether a technology will pass constitutional muster. Fingerprinting, the Court noted, citing *Davis v. Mississippi*, did not involve "probing into an individual's private life and thoughts that marks an interrogation or search."[98] In a sense, this determination exculpates all biometric surveillance technology—law enforcement officials can simply say that biometrics serve only to determine whether or not a particular individual is a criminal or is carrying contraband. The limited nature of the search can thus be justified, and in general the limited scope of the inquiry makes it more likely that a particular technology—such as pen registers that only record the number dialed from a phone but does not record the content of conversations—will be ruled constitutional.[99]

23. The nature of the search is limited because it is a binary search. FaceIt generates a face print and compares it to files in its database of wanted criminals—and, according to company officials, discards the computerized print from its memory if there is no match.[100] In this way, all FaceIt really does is answer a simple question: Is the individual being scanned a criminal? The software answers the question as either yes or no—there is no inquiry into the person's privacy in the realms that have traditionally been held to be within the parameters of personal privacy including matters of health, sexuality, personal information (aside from identity), decisional privacy, and financial privacy. In other words, the scope of the search might be argued to be non-testimonial and hence would not implicate any privacy rights.

24. Indeed, FaceIt very closely resembles metal detectors at airports or dog sniffs that the Court has held constitutional in *United States v. Place* where no search warrant or probable cause was present,[101] or a test by law enforcement officials of white powder to determine whether or not it was cocaine as opposed to sugar or talcum powder[102] which the court held constitutional in *United States v. Jacobsen*.[103] In *Place*, the court noted that the limited, binary nature of a "canine sniff" did not qualify as a "search" implicating the Fourth

---

[98] Dionisio, 410 U.S. at 15 (citing Davis v. Mississippi, 394 U.S. at 727). "Nor can fingerprint detention be employed repeatedly to harass any individual, since the police need only one set of each person's prints. Furthermore, fingerprinting is an inherently more reliable and effective crime-solving tool than eyewitness identifications or confessions and is not subject to such abuses as the improper line-up and the 'third degree.'" *Id.*

[99] Smith v. Maryland, 442 U.S. 735 (1979).

[100] "If a face matches above a certain confidence level, it sounds the alarm. If a face does not match, there's no memory; it does not get stored, it does not get added to a database." Joseph Atick, as quoted on *Analysis: Police, Video Surveillance and Privacy*, NATIONAL PUBLIC RADIO: TALK OF THE NATION, July 16, 2001, available at http://search.npr.org/cf/cmn/cmnpd01fm.cfm?PrgDate=07/16/2001&PrgID=5.

[101] United States v. Place, 462 U.S. 696 (1983).

[102] United States v. Jacobsen, 466 U.S. 109 (1984). In this case, workers on a private freight carrier noticed white powder being stored in a damaged cardboard box and called federal agents who then removed a trace of the powder and determined that it was cocaine. In upholding the convictions, the Court noted that, "a chemical test that merely discloses whether or not a particular substance is cocaine does not compromise any legitimate interest in privacy." *Id.* at 123.

[103] *Id.* at 122.

Amendment at all.[104] Such a sniff did not require "opening the luggage" or the exposure of non-contraband items.[105] The sniff only reveals "the *presence or absence* of narcotics, a contraband item" (emphasis added).[106] Though the court noted that—in 1983—it knew of "no other investigative procedure that is so limited both in the manner in which the information is obtained and in the content of the information revealed by the procedure,"[107] it is clear that FaceIt is precisely such a technology. FaceIt reveals no "intimate details" which courts have held as an important factor in determining the constitutionality of surveillance technology.[108] In sum, the three factors mentioned above are all in favor of allowing FaceIt pass through the constitutional filter.

V. WHAT NOW? THE NEED FOR PROTECTION FROM THE GAZE IN PUBLIC

25. The Supreme Court has intimated in the past that citizens enjoy the right to "dwell in reasonable security and freedom from surveillance."[109] But two problems are evident with respect to FaceIt technology: First, the declining freedom to be free from surveillance is not in the home, but the public plaza.[110] While Courts have regulated surveillance of the home rather vigorously, surveillance in public places has not really been opposed constitutionally. Secondly, dicta of the Court are simply too weak in order to bar, on constitutional grounds, such technologies that are as powerful and able to be used in public, without intrusion, as FaceIt. This section will outline the various arguments for the need for constitutional protection against such facial recognition software such as FaceIt.

---

[104] Place, 462 U.S. at 707.

[105] *Id.* ("A 'canine sniff' by a well-trained narcotics detection dog, however, does not require opening the luggage. It does not expose noncontraband items that otherwise would remain hidden from public view, as does, for example, an officer's rummaging through the contents of the luggage.")

[106] *Id.*

[107] *Id.* Do canine sniffs enhance or replace an officer's senses which he was born with? The rule of thumb that technology enhancing senses tend to pass Fourth Amendment scrutiny (*see* Texas v. Brown, allowing the use of a flashlight to look into the back of suspect's car), and technology replacing senses failing it (*see* Kyllo, barring the use of thermal imaging technology), seems to break down a bit here. Justice Brennan, in a concurrence, raised precisely this point: "Unlike the electronic 'beeper' in *Knotts*, however, a dog does more than merely allow the police to do more efficiently what they could do using only their own senses. A dog adds a new and previously unobtainable dimension to human perception." *Id.* at 719.

[108] *See*, *e.g.*, supra, note 63. The Dow Chemical Court noted that use of technology should not be barred and that government should not be "foreclosed from using technology to enhance its surveillances, provided that that technology does not reveal 'intimate details.'" 476 U.S at 238. This intimate details test, however, has been criticized severely for its ambiguity. Which facts are "intimate" and which ones are not? Another problem is that such determination can only be made *after* a search has already been conducted. "Without a bright-line standard, law enforcement has no way to know what conduct is proscribed before a search is conducted. The unacceptable result is that Fourth Amendment issues are being decided by an ex post facto review of whether the search turned up 'alarmingly personal information'—rather than whether the activity itself constitutes a search." McKnight, *supra* note 80 at 1259 (1999).

[109] Johnson v. United States, 333 U.S. 10, 14 (1948).

[110] "The real threat lies in the systematic monitoring of public places, where ability and legality have created a surveillance free-for-all… Whereas we have a reasonable expectation of privacy in our own homes, there is no longer such an expectation for public places." GARFINKEL, *supra* note 16, at 93.

A. THE BIG CHILL

26. FaceIt has the ability to implement what has to this day only existed in the mind of George Orwell or Michel Foucault who described the Panopticon as a prison in which inmates could not be sure if they were being watched or not, only that they *could* be watched; as a result their behavior was deterred and conformity was thus coerced.[111] There is little empirical data, to be sure (mostly because there are almost no case studies of this), but courts, policy makers, journalists and general citizens have commented on the potential "chilling effect" of such omnipresence of cameras—arguing that their presence will deter even legal behavior because citizens are afraid of accidentally violating the law.[112] The original American Bar Association standards on physically assisted surveillance commented on this "chilling effect" and sought to require regulation of technology; in an early draft it noted that regulation was needed when such surveillance would pose "a significant infringement of other widely shared values in a democratic society, including the enjoyment of anonymity… the absence of a pervasive police presence, and the absence of intensive official scrutiny except in response to suspicious conduct."[113] In many ways, the perception of privacy is as important as substantive privacy and law enforcement should do everything it can in order to protect it. "When people fear surveillance, whether it exists or not, when they grow afraid to speak their minds and hearts freely to their government or to anyone else, then we shall cease to be a free society."[114] And even more on point: "A bathtub is a less private area when the plumber is present even if his back is turned."[115] This last dicta, written by Justice Stevens in Karo, highlights the nature of the privacy interest involved if we engage in a little thought experiment: Would the same bathtub be less private if the plumber were to wear a blindfold, earplugs and were not allowed to move around? The answer most would give—that privacy would still somehow be implicated—would show that privacy interests in many regards is a *subjective* perception—thus it would not matter if citizens were being watched—the mere perception that they are is erosive of privacy and government officials ought to take this into account when deciding to implement such technology.

27. Presumably, the prominent presence of cameras could chill even legal behavior. Courts have often looked to the policy implications such as a "chilling effect" of legal behavior when making their decisions; however, it has usually been treated as a factor among many other factors, not as a dispositive factor in itself.[116] In *Younger v. Harris*, for example, the Court noted that a chilling effect does not "by itself justify federal intervention."[117] Courts have struck down laws and ordinances for being "void for vagueness" because they chill legal behavior. In *Papachristou v. City of Jacksonville*, for example, the Court struck down

---

[111] Jeremy Bentham first described this ring-shaped prison in which inmates were always under surveillance. In the center of the prison would be an inspection tower with windows facing the inner wall of the ring. Supervisors in the center room would see every cell, but inhabitants of the rooms would not see the inner room. As a result, they could never be sure whether, at any one time, they were being watched. As a result, their behavior would be checked and deterred. MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON (Alan Sheridan trans., Vintage Books 2d ed. 1995) (1977).
[112] *See, e.g.*, Rosen, *A Cautionary Tale for a New Age of Surveillance*, N.Y. TIMES, Oct. 7, 2001.
[113] Slobogin, *supra* note 85, at 430.
[114] Senator Ervin, as quoted in, ARYEH NEIER, DOSSIER: THE SECRET FILES THEY KEEP ON YOU 14 (1975).
[115] 468 U.S. at 735.
[116] *See, e.g.*, Bartnicki v. Vopper, 532 U.S. 514 (2001).
[117] Younger v. Harris, 401 U.S. 37, 50 (1971).

an ordinance against vagrants because a vague statute could prevent a person of ordinary intelligence from conforming with legal conduct since he or she would not be able to determine what was legal. The resulting self-restraint would cut down on legal behavior as well. Secondly, a vague ordinance would place allow police to enforce the ordinance arbitrarily.[118] But in the case of FaceIt, there are no ordinances, and so such Court intervention is unlikely.

B. MISSION CREEP AND THE POTENTIAL FOR ABUSE

28. Even though company officials have taken steps to minimize privacy intrusions—face prints of innocent citizens are discarded, for example—the potential for abuse is still vast. Allowing FaceIt technology would establish the infrastructure that would make abuse both possible, and very easy. Law enforcement officials could watch not only criminals, but also political dissidents. Because the computer databases against which face prints are matched can be interchanged, this would be a very simple operation. Secondly, company officials have argued that individuals are only identified and not tracked, but have also admitted that FaceIt technology has such capabilities.[119] If this is the case, then tracking, or following individuals would be a very easy matter. Authorities can simply enter a person's face print and "reverse engineer" the identity of these individuals, by searching data from previous movements—to see who they have met with, what they have done, and so on.[120]

29. There are currently features that control against such abuse—face prints, according to officials, are immediately discarded if no match is made.[121] Nevertheless, history has shown that "mission creep"[122] has occurred in the past—technology or structures set up for one purpose ultimately are used for another purpose. For example, American-made cameras ostensibly installed for traffic control in China's Tiananmen Square were eventually used to find and arrest subversives after the protests in 1989.[123] But one does not have to look to Communist China in order to find this mission creep. In America, examples of such mission creep abound—the most famous of which is the social security number. The number was created only for use in conjunction with the Social Security system itself, but the use of the number soon went further.[124] In 1943, the number was used as a permanent account number; in 1961 the Internal Revenue Service made it into the universal taxpayer identification number. Soon Social Security numbers featured prominently on driver's licenses, military personnel files, Treasury bonds, health benefits, welfare, and bank accounts.[125] Social Security numbers are even used in some law school examinations for fair grading. If FaceIt

---

[118] Papachristou v. City of Jacksonville, 405 U.S. 156 (1972).
[119] *See* http://www.visionics.com.
[120] John Woodward, Jr., *Super Bowl Surveillance: Facing up to Biometrics,* 2001 RAND ARROYO CTR 8, *available at* http://www.rand.org/publications/IP/IP209/IP209.pdf (last visited Apr. 15, 2002).
[121] Joseph Atick, on *Analysis: Police, video surveillance, and privacy*, NPR: TALK OF THE NATION, July 16, 2001. "If a face does not match, there's no memory; it does not get stored, it does not get added to a database." [Transcript on file with the author.]
[122] Woodward, *supra* note 120, at 13.
[123] SYKES, *supra* note 47, at 36.
[124] *Id.* at 51.
[125] *Id.* at 52.

can be used to scan for terrorists, there is little to stop authorities from using it to track deadbeat dads or people with overdue library books, or even more nefarious purposes.[126]

C. GUILTY UNTIL PROVEN INNOCENT: THE PROBLEM OF SUBJECTING EVERYONE TO A SEARCH.

30. If the information sought by FaceIt is not over-inclusive (the system only seeks to confirm or deny whether or not a face belongs to a known criminal), FaceIt is nevertheless over-inclusive in another way, and this is an additional reason why FaceIt makes ordinary citizens uneasy: The system subjects *everyone*, including innocent citizens, to indiscriminate scrutiny. The *Dow Chemical* court noted in a dissent that, "The Fourth Amendment protects private citizens from arbitrary surveillance by their Government."[127] This was true even though the search at issue was a fly-over not implicating any intrusion—in fact, it is quite possible that defendants did not even know that this fly-over had ever happened. In this sense, FaceIt technology would be the same. Other courts have raised a similar issue: In a passionate dissent in *Olmstead* that allowed for wiretapping as long as no physical trespass had taken place, Justice Brandeis argued that "the tapping of one man's telephone line involves the tapping of the telephone of every other person whom he may call, or who may call him. As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wiretapping."[128] Congress has also enacted, in their crime enforcement legislation, provisions that minimize or eliminate the recording of innocent citizens, even though, for example, law-abiding citizens accidentally caught on tape are not identified or imposed upon. In allowing video surveillance, a court interpreted the minimization requirement of the Title III of the Omnibus Crime Control and Safe Street Act of 1968 to say that the law did not forbid the interception of non-relevant matter, but that such matter was to be kept at a minimum.[129]

31. That technology such as FaceIt has dramatically shaken the frame of reference with which the Fourth Amendment must be interpreted is also evident in the dissent in *Ciraolo*. On the one hand, the dissent argued that, "comings and goings on public streets are public matters, and the Constitution does not disable police from observing what every member of the public can see."[130] Yet elsewhere, the dissent asserts that police observation from an airplane ought to be unconstitutional since travelers are likely to look into defendant's backyard only for a short time, the implication being that they could hence not really identify the marijuana in the backyard. In this sense, the dissent sought to draw a line between looking and looking *for*.[131] Clearly, the implications of FaceIt technology raises the same tension—on the one hand, FaceIt technology only targets the "comings and goings on public streets;" on the

---

[126] Woodward, *supra* note 120, at 13.
[127] Dow Chemical, 476 U.S. at 240.
[128] Olmstead, 277 U.S. at 476.
[129] 18 U.S.C.A. §§ 2510-2520.
[130] Ciraolo, 476 U.S. at 224.
[131] "The Court's holding, therefore, must rest solely on the fact that members of the public fly in planes and may look down at homes as they fly over them. […] This line of reasoning is flawed. First, the actual risk to privacy from commercial or pleasure aircraft is virtually nonexistent. Travelers on commercial flights, as well as private planes used for business or personal reasons, normally obtain at most a fleeting anonymous, and nondiscriminating glimpse of the landscape and buildings over which they pass." *Id.* at 223.

other hand, citizens walking are not given "fleeting anonymous, and nondiscriminating"[132] glimpses, but they are looked at and identified.

D. THE PROBLEM OF SCALE: QUANTITATIVE DIFFERENCES BECOME QUALITATIVE DIFFERENCES

32. Even if a certain technology is constitutional, its application on a vast scale might still raise constitutional concerns. This point has already been expressed with respect to a relatively innocuous technology—the "dog sniff". Having held in *Place* that dog sniffs were constitutional, Justice Brennan noted in a passionate dissent that the widespread and indiscriminate use of such dog sniffs might imply constitutional problems. His imploration was very passionate and will be excerpted in large here:

> Before excluding a class of surveillance techniques from the reach of the Fourth Amendment, therefore, we must be certain that none of the techniques so excluded threatens the areas of personal security and privacy that the Amendment is intended to protect… It is certainly true that a surveillance technique that identifies only the presence or absence of contraband is less intrusive than a technique that reveals the precise nature of an item regardless of whether it is contraband. But by seizing upon this distinction alone to conclude that the first type of technique, as a general matter, is not a search, the Court has foreclosed any consideration of the circumstances under which the technique is used, and may very well have paved the way for technology to override the limits of law in the area of criminal investigation. For example, under the Court's analysis in these cases, law enforcement officers could release a trained cocaine-sensitive dog—to paraphrase the California Court of Appeal, a 'canine cocaine connoisseur'—to roam the streets at random, alerting the officers to people carrying cocaine. Or, if a device were developed that, when aimed at a person, would detect instantaneously whether the person is carrying cocaine, there would be no Fourth Amendment bar, under the Court's approach, to the police setting up such a device on a street corner and scanning all passersby. In fact, the Court's analysis is so unbounded that if a device were develop that could detect, from the outside of a building, the presence of cocaine inside, there would be no constitutional obstacle to the police cruising through a residential neighborhood and using the device to identify all homes in which the drug is present… Hence, at some point in the future, if the Court stands by the theory it has adopted today, search warrants, probable cause, and even 'reasonable suspicion' may very well become notions of the past.[133]

---

[132] *Id.*

[133] Place, 466 U.S. at 138.

33. It is the application of constitutionally legal surveillance technology on this vast scale that itself raises constitutional issues. It is true, as A. Michael Froomkin has argued, that moving in public is not truly anonymous even though one enjoys the illusion of privacy and anonymity—others may recognize you and someone might jot down the license plate number of your car.[134] "That freedom is soon to be a thing of the past, as the 'privacy commons' of public spaces becomes subject to the enclosure of privacy-destroying technology."[135] The scale problem is aggravated by the creation of the computerized database that can handle vast amounts of data using very few resources. In 1965, a Congressional Special Subcommittee on Privacy was established, but it was at first only concerned about personnel matters (and the process by which the personnel would be recruited and tested), not with computers, at least until proposals for a National Data Center were floated.[136]

VI. RE-READING THE FOURTH AMENDMENT: GOVERNMENT ACCOUNTABILITY

34. Justice Brennan's long dissent in *Jacobsen* was highly prescient in its prediction that notions of "reasonable suspicion" might become notions of the past with the forward march of technology. FaceIt threatens to make any and all forms of suspicion obsolete because every face in public is scanned. It is time, therefore, to perhaps re-conceptualize the Fourth Amendment and to consider what it is meant to protect and if a scan by FaceIt might still be a search even though current jurisprudence suggests otherwise. In *Code: and Other Laws of Cyberspace*, Lawrence Lessig argues that there are different conceptions of what the Fourth Amendment protects.[137] Lessig argues that the Fourth Amendment could be read as maximizing utility, as protecting dignity or as containing a substantive right to privacy that limits government power. In the past, the Fourth Amendment protected all three, as all three coincided whenever there was a search.[138] Thus, for example, in one of the most famous early search-and-seizure cases, John Wilkes had used the press to communicate with his constituents and criticize George III of England.[139] The government reacted by breaking into his house and rummaging through his papers. Under Lessig's conception, utility was affected (the British forces created a mess and otherwise destroyed some of the property), dignity was affected (the search disrespected Wilkes's rights to privacy), and his substantive privacy was diminished in inverse proportion to the government's exercise of power. But technology changes all that, and the three aims of the Fourth Amendment do not coincide all the time: it is possible to have a search that is not detectable.[140] This article will argue that a full consideration of the Fourth Amendment, coupled with the advances in technology, favors an approach to protect substantive privacy.

---

[134] A. Michael Froomkin, *The Death of Privacy?* 52 STAN. L. REV. 1461 (2000).
[135] *Id.*
[136] MALCOLM WARNER AND MICHAEL STONE, THE DATA BANK SOCIETY: ORGANIZATIONS, COMPUTERS AND SOCIAL FREEDOM 83 (1970).
[137] LAWRENCE LESSIG, CODE: AND OTHER LAWS OF CYBERSPACE 111 (2000).
[138] *Id.* at 149.
[139] AKHIL REED AMAR, THE BILL OF RIGHTS: CREATION AND RECONSTRUCTION 65 (1998), citing Wilkes v. Wood, 98 Eng. Rep. 489 (C.P. 1763).
[140] "Now that technologies such as the worm can search without disturbing, there is a conflict about what the Fourth Amendment protects." LESSIG, *supra* note 137, at 149.

A. UTILITY CONCEPTION: IF A TREE FALLS IN THE FOREST…

35. One conception of the Fourth Amendment is the "utility conception"[141]—the point of this interpretation is that the protection seeks to minimize intrusion. Having police officers go into one's house, open drawers, read journals, overturn mattresses, and pry up floorboards is very burdensome to the individual. In this way, what is really protected is the citizen's right to peace. "The test then is the burden of the state's intervention; when an intervention can be made less burdensome, the protection against it decreases as well."[142] The Court seems to have adopted this standard, and as has been seen, against technology such as FaceIt that does not at all interfere with utility—indeed, individuals do not even know their faces have been scanned. Under this conception, as the intrusion sinks to zero, the Fourth Amendment protection falls to zero as well. If the police look around your place, and you do not notice it, has a search still taken place? The utility conception would argue no, and hence this view provides little opposition to technologies such as FaceIt.

B. A MATTER OF PRINCIPLE: GUILTY UNTIL PROVEN INNOCENT?

36. The second conception that Lessig proposes looks at how individual *dignity* is affected by a particular search. Regardless of how intrusive a search is, normatively, a search normatively offends dignity—whether because of the implication of criminal liability, privacy concerns, or other issues. Under this conception, the search—even one that physically does not impose, violates the Fourth Amendment because it is, in essence, a fishing expedition. The government assumes that everyone is guilty and scans everyone's face until evidence (lack of a file in the database) proves otherwise.

37. Thus, "it is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty and private property" that is at the heart of the Fourth Amendment.[143] This conception is more on point—indeed to have one's face scanned and compared against a database of known criminals is somewhat deprecating of dignity in principle, but because *everyone* is scanned, this argument is not as likely to stand up against FaceIt.

C. FOURTH AMENDMENT'S GOVERNMENT ACCOUNTABILITY REQUIREMENT: THE LIGHT AT THE END OF THE TUNNEL?

38. The third and final conception of the Fourth Amendment that Lessig proposes is that there is a right to substantive privacy—not to protect the individual, but to *constrain government power*. "Understood this way, privacy does more than protect dignity or limit intrusion; privacy limits what government can do."[144] Other scholars, such as Jed Rubenfeld, have advanced this line of argument as well.[145] Under this conception, allowing sensory

---

[141] *Id.* at 146.
[142] *Id.* at 146.
[143] Boyd v. United States, 116 U.S. 616, 630 (1886).
[144] LESSIG, *supra* note 137, at 149.
[145] "The right to privacy has everything to do with delineating the limits of governmental power." In arguing that *Bowers v. Hardwick* was really a case about homosexual intimacy rather than homosexual sex, Rubenfeld argues that "where our identity or self-definition is at stake, there the state may not interfere." Rubenfeld, *The Right of Privacy*, 102 HARV. L. REV. 737 (1989).

enhancing devices defeats this aim of the Fourth Amendment. "At what point does one voluntarily expose something: when the government can discover it by using binoculars; by looking over a fence; by looking from an airplane?"[146] The Fourth Amendment's protection of the citizenry and the limitation of power of the government usually coincide, but with advances in technology, emphasis must be placed on the latter. "Uncontrolled search and seizure is one of the first and most effective weapons in the arsenal of every arbitrary government."[147]

39. What Lessig does not address, but what this article will point out, is that in general, the Fourth Amendment has held that searches have to be accompanied by a warrant. The Supreme Court has, in many instances, pointed to this requirement as well.[148] "A search is 'unreasonable' unless a warrant authorizes it, barring only exceptions justified by absolute necessity."[149] There are less restrictive standards such as probable cause or reasonable suspicion, but to some degree *some* inkling triggering a search has to be present. To a large extent, this requirement is meant to make government accountable in its searches of citizens.

40. One major part of this accountability requirement is the Fourth Amendment's emphasis on reasonableness. Thus, law enforcement officials have to *explain* to the citizen the reasons for the search. Whenever applying for a warrant, law enforcement officials have to describe, among other things and in detail, the following: the place to be searched, the persons to be seized, the property to be seized.[150] While the specificity requirement of the warrant is intended to help officers execute the warrant without civil rights violations,[151] and while it may appear that the requirements are meant to increase police efficiency—describing the people to be searched accurately makes for quicker identification and easier seizure—one cannot ignore that these requirements are meant to require government accountability: After all, even if the officer on the case is about to make a bust, he has to get a warrant. Surely the officer is already familiar with how the suspect looks and what he needs to be seized—the warrant will not in any way help him seize the correct person. Here it seems that the warrant serves, at least in part, to create a paper trail that a judge or citizens can later examine for purposes of determining whether or not the search was reasonable. Thus, if the government

---

[146] Thomas Clancy, *What does the Fourth Amendment Protect: Property, Privacy, or Security?*, 33 WAKE FOREST L. REV. 307, 366 (1998).
[147] Justice Jackson, dissenting in Brinegar v. United States, 338 U.S. 160 (1949).
[148] *See, e.g.*, Mincey v. Arizona, 437 U.S. 385 (1978) and Coolidge v. New Hampshire, 403 U.S. 443 (1971).
[149] United States v. Rabinowitz, 339 U.S. 56, 70 (1950) (Frankfurter, J., dissenting).
[150] AMERICAN BAR ASSOCIATION, CRIMINAL JUSTICE SECTION. GUIDELINES FOR THE ISSUANCE OF SEARCH WARRANTS 30 (1990) ("The Fourth Amendment requires that the warrant describe the place to be searched and things to be seized with reasonable particularity. Warrants which fail to do so are condemned as 'general' or 'exploratory' as they do not give the searching party sufficient direction. Because they permit fishing about for evidence, unnecessary invasions of privacy result.").
[151] On first inspection, it seems that the specificity requirements are intended to help police officers to find the contraband, and that the requirements are for purposes of efficiency only: "The description of the premises, vehicle, or container to be searched should be sufficiently specific so that an officer with reasonable effort can find it… individuals to be seized and searched must be described with enough specificity to enable the police officers executing the warrant to identify them with reasonable certainty." *Id.* at 32.

fails to explain the goals of a search beforehand with a reasonable amount of specificity, the Court will often find a Fourth Amendment violation.[152]

41. Although this view is not completely without its critics, the general consensus has been that the more intrusive a search, the higher the justification standard has to be.[153] In searching someone's house (very intrusive), police need a warrant signed by a judge. But in patting someone down (less intrusive), cops only need a reasonable suspicion—nevertheless, the suspicion has to be individualized.[154] Regardless, citizens know when they are patted down and can therefore directly inquire as to the reason for which they are searched. But that leaves the question: If a search is not intrusive at all, do police officers still need some kind of even *de minimis* suspicion? *Kyllo* failed to really answer this, but it would seem that under Lessig's conception of the Fourth Amendment as limiting government power and requiring accountability, some suspicion is still needed.

42. Perhaps what is important in the Fourth Amendment is not so much whether a house is being searched, but whether a house is being searched *without reason*—so the burden is on the government to justify the search. If this is true, suspicionless searches without any justification might be unconstitutional because they are arbitrary. FaceIt then, under this conception, would allow police to scan faces without justification, and so a court might hold the technology unconstitutional because it would "allow for a dangerous amount of police discretion, [and] because these [sense enhanced] searches eviscerate the traditional requirement that police identify a particular suspect prior to initiating a search."[155] Biometric surveillance technology such as FaceIt has often been praised for being non-intrusive to the citizen.[156] But this non-intrusiveness is precisely the problem. The warrant requirement has been watered down in some circumstances depending on other factors such as intrusiveness of search, for instance.

43. Nevertheless, *individualized notice* has not been a problem with these other types of searches. A very plausible reading of the Fourth Amendment would imply that the warrant

---

[152] *See, e.g.*, Lo-Ji Sales, Inc. v. N.Y., 442 U.S. 319 (1979) (holding that a search of an adult bookstore in which officials seized several films and magazines was a Fourth Amendment violation because the warrant issued did not describe the things to be seized).

[153] For a cogent critic of the view that the Fourth Amendment contains a warrant requirement, *see*, Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757 (1994). Amar argues that the Fourth Amendment does not require a search warrant. Because the Fourth Amendment only states that "*no* warrant shall issue, but upon probable cause," he takes it to mean that only those warrants that are issued, shall pass a probable cause filter. Amar argues that the Bill of Rights is actually silent on other searches. Furthermore, a close historical analysis of the warrants shows that warrants were actually not the constitutional checks against authority that they are often thought to be today. In fact, they were a tool for the oppressors—and judges issued them liberally, to the dismay of the citizenry. "Warrants then, were friends of the searcher, not the searched." Despite Amar's intriguing analysis, this article argues that even if Amar were correct, the warrant requirement today, as confirmed by the Supreme Court on repeated occasions, along with the restraining nature of the warrant in modern times on law enforcement, merits its acknowledgement and enforcement. For a criticism of Amar, see Carol Steiker, *Second Thoughts about First Principles*, 107 HARV. L. REV. 820 (1994).

[154] Ybarra v. Illinois, 444 U.S. 85, 91 (1979).

[155] David Steinberg, *Making Sense of Sense-Enhanced Searches*, 74 MINN. L. REV. 563, 569 (1990).

[156] Joseph Atick, *Computerized Facial Recognition: A Technology with Broad Range of Real-World Applications*, Testimony before the U.S. House of Representatives Comm. on Banking and Fin. Servs., (May 20, 1998), *at* http://www.house.gov/financialservices/52098dja.htm.

requirement seeks to balance minimization of intrusion and notice at the same time. In other words, the warrant requirement has two goals. The first goal is that the more intrusive a search is, the more justification is needed—hence a warrant is required for raiding someone's house, but none is needed for a pat down. However, the second goal is notice: A warrant also serves as a notice that a search is authorized and is occurring. In the past, notice was incidental to a search—the subject of the search always knew that he had been searched, whether the clothes in his apartment were strewn about the apartment or whether a police officer was patting him down. Relaxing the warrant requirements in these instances comported with the Fourth Amendment in that both justification and notice were served: The plain view exception, for example, did not require a warrant because residents always saw when the police officer, responding to a domestic violence call for example, seized narcotics that were in plain view. Similarly, a search of an area subject to the immediate control of a person arrested is also commonly accepted, again because the person being arrested knew of the police presence and could see them search a bag that he was carrying with him at the time.[157] Warrantless searches can also occur in instances where the individual has actively given up control of a certain property—when a suspect has abandoned property, for example[158]—but this is inapplicable to FaceIt technology, for a person cannot be said to have abandoned his face, because such a citizen cannot easily hide his face in public—he cannot show a subjective expectation of privacy in his face.

44. Notice was never a problem, until technology encroached—and when it did, as it did in Katz for example, courts immediately imposed a warrant requirement. With FaceIt technology—identification at a distance—no notice is ever given that a search has been conducted. "Without this notice, warrantless searches could be conducted with practically no government accountability."[159] In order to combat this abuse, as a search becomes non-intrusive, the burden on law enforcement officials to explain or justify their search ought to be even *higher* than for a search in which subjects become aware that they are being searched. This heightened justification requirement would be in a way to compensate for the reduced notice that traditionally was incidental to the search itself. "An electronic frisk should have to meet a legal standard higher than that of a physical frisk."[160] Under this conception, mutual transparency would be required.[161]

VII. ANONYMITY AS GAP-FILLER?

45. These potential Fourth Amendment-based arguments against FaceIt are mostly based on dicta or extrapolation, and therefore offer very weak opposition to technology such as

---

[157] *See*, for a survey of situations in which searches can be done without warrants, PROJECT ON LAW ENFORCEMENT POLICY AND RULEMAKING, MODEL RULES: WARRANTLESS SEARCHES OF PERSONS AND PLACES (1974). *See*, for further case law, Chimel v. California, 395 U.S. 752 (1969) (allowing searches incidental to arrest in the areas within arrestee's immediate control, i.e. the area from which he might draw a weapon or within which he might destroy evidence), and United States v. Becker, 485 F.2d 51 (6th Cir. 1973).

[158] MODEL RULES: WARRANTLESS SEARCHES OF PERSONS AND PLACES, at 42. This abandonment doctrine is an outgrowth of the plain view doctrine: "By abandoning the property, the owner has lost any reasonable expectation of privacy, as any member of the public might come by and retrieve or examine it."

[159] McKnight, *supra* note 80, at 1263.

[160] Rosenberg, *supra* note 87, at 156.

[161] *See*, *e.g.*, DAVID BRIN, THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM? (1998).

FaceIt. Even though the arguments are intellectually interesting, to contend that the Fourth Amendment would prohibit the use of technology such as FaceIt is simply to fight an quixotic battle, and it might take too long for courts to reformulate a new conceptualization of the Fourth Amendment to protect citizens against FaceIt. Instead, one must realize that the expectation of privacy has crumbled with the onslaught of technology, and it might be time to turn to another potential—and more immediately available—source of opposition to FaceIt technology. That source is anonymity.

46. If technology has eroded the expectation of privacy, one could argue that courts have consistently upheld what might be termed the expectation of anonymity. The definition of privacy is almost certainly too broad in order to meaningfully protect individuals against FaceIt. "'Privacy' has become as nebulous a concept as 'happiness' or 'security.'"[162] To simply say that FaceIt violates privacy by infringing on the "right to be left alone",[163] for example, is not useful because in the FaceIt case, the people being scanned are technically being left alone. "The great simplicity of this definition gives it rhetorical force and attractiveness, but also denies it the distinctiveness that is necessary for the phrase to be useful in more than a conclusory sense."[164] As a spokesman for the Tampa Police department stated after the use of video surveillance at the Super Bowl: "There is no expectation of privacy in a crowd of 100,000 people."[165] Such a definition of privacy exempts biometric surveillance because proponents can simply claim that such technology leaves citizens alone while ignoring the argument that privacy claims also have to do with, for example, an individual's reluctance to have a file in a database or to have his or her face scanned unknowingly. Anonymity is a much narrower conception of the value at stake insofar as biometric technology is concerned. While there may be no expectation of privacy in a crowd, there may be an expectation of anonymity in such a space.[166] Because this technology is primarily concerned with identification rather than searches, anonymity is a value that is tailored much more narrowly and is therefore better equipped to deal with biometric surveillance.

47. Privacy is closely allied with anonymity. "We may commute for years—same train, same compartment, same fellow-travelers—and yet the man to whom we reveal our hopes, our opinions, our beliefs, our business and domestic joys and crises remains 'The chap who gets on at Dorking with *The Times* and a pipe; I don't know who he *is*.' And he does not know who we *are*, because we have never exchanged names, and thus the necessary communication and release of our private concerns is accomplished without violation of our privacy. *In our anonymity is our security*."[167] But the value of anonymity is its role as buffer to privacy intrusions. In other words, "we will tolerate considerable intrusion, and even volunteer supererogatory circumstantial detail of our lives, if our anonymity is preserved."[168]

---

[162] Raymond Wacks, *The Poverty of 'Privacy'*. THE LAW QUARTERLY REVIEW (1980).
[163] Samuel Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).
[164] Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421 (1980).
[165] Daryn Kagan, *Cameras Inspected Super Bowl Crowd for Criminals*, CNN MORNING NEWS, Feb. 1, 2001. [Transcript on file with author.]
[166] Alan Westin, *Science, Privacy, and Freedom: Issues and Proposals for the 1970's*, 66 COLUM. L.REV. 1003 (1966).
[167] WARNER, *supra* note 136, at 126.
[168] *Id.*

A. ANONYMITY HAS BEEN UPHELD ESPECIALLY IN PUBLIC SPACES.

48. The strength of using anonymity to oppose FaceIt rather than expectations of privacy lies in the fact that courts have generally protected anonymity in *public spaces* whereas they have in general held that there is no expectation of privacy in public places. This is because anonymity has implications for the First Amendment and has strong political dimensions, from the earliest beginnings of the country. The Federalist papers of Alexander Hamilton, James Madison and John Jay were published anonymously, under the pen name of "Publius."[169] Over the years, at least six presidents, fifteen cabinet members, and thirty-four congressmen published anonymous political writings.[170] In *McIntyre v. Ohio Elections Com'n*, the court indicated in striking down an ordinance requiring that political pamphlets bear the name of the author that:

> Under our Constitution, anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and of dissent. Anonymity is a shield from the tyranny of the majority [citing J. Mill, On Liberty]. It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation—and their ideas from suppression—at the hand of an intolerant society. The right to remain anonymous may be abused when it shields fraudulent conduct. But political speech by its nature will sometimes have unpalatable consequences, and, in general, our society accords greater weight to the value of free speech than to the dangers of its misuse.[171]

49. In *Thomas v. Collins*,[172] the Court held that the president of the United Auto Workers did not have to register as a labor organizer with the Secretary of State in Texas before being able to identify himself as such on business cards and solicit new members. "Although the ambiguities in the *Thomas* opinion leave its scope in doubt, it may be read as a recognition of a right of anonymity."[173] The Court has also upheld the refusal of individuals to disclose the names of individuals who had bought defendant's book,[174] the refusal of party officials to divulge the names of other members of the Progressive Party[175] and the refusal of a witness to reveal to the House Committee on Un-American Activities if other individuals had participated in the Communist Party.[176] The right to anonymity was even more firmly expounded on in *NAACP v. Alabama ex rel. Patterson*[177] in which the Supreme Court upheld the refusal of the NAACP to disclose its membership lists because to do so would be

---

[169] *See, e.g.,* ALEXANDER HAMILTON, JAMES MADISON AND JOHN JAY, THE FEDERALIST PAPERS. (Clinton Rossiter ed., Mentor 1999) (1788).
[170] SYKES, *supra* note 47, at 85.
[171] 514 U.S. 334, 357 (1995). *See also*, Talley v. California, 362 U.S. 60 (1960). "Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind." 362 U.S. at 64.
[172] 323 U.S. 516 (1945).
[173] *Note: The Constitutional Right to Anonymity: Free Speech, Disclosure and the Devil*, 70 YALE L.J. 1084, 1094 (1961).
[174] United States v. Rumely, 345 U.S. 41 (1953).
[175] Sweezy v. New Hampshire, 354 U.S. 234 (1957).
[176] Watkins v. United States, 354 U.S. 178 (1957).
[177] 357 U.S. 449 (1958).

a violation of the associational privacy implied by the First Amendment. And in *Shelton v. Tucker*[178] the Court struck down a statute requiring teachers to list their group affiliations on an annual basis. Despite this line of cases, the scope of anonymity has not really been specified.[179] This term, the Supreme Court will hear *Watchtower Bible & Tract Soc. of New York, Inc. v. Village of Stratton*,[180] in which Jehovah's Witnesses are challenging the constitutionality of an ordinance that requires door-to-door proselytizers to register first.

50. Courts have further upheld anonymity in another prominent public forum: The Internet.[181] Various scholars have decried the fact that cookies and other technology are eroding anonymity on the Internet.[182] Individuals and organizations have argued, and courts have agreed, that there is a strong interest in being anonymous on the Internet because in the discussion of sensitive topics, they would like to avoid "ostracism or embarrassment."[183] In some cases, scholars have even argued, anonymity might even change race relations.[184]

51. Internet anonymity is easy to come by—unlike anonymity off-line. Instead of having to go outside to find a payphone and making a call using a disguised voice, now users could simply find a re-mailer service that would ensure anonymity. "One of the most valuable democratic aspects of the Internet is its capability for anonymous communication."[185] Thus, it is evident that anonymity is a fundamental right that courts have in general been very aggressive in protecting and it is this right that might offer a foundation for constitutional protection against FaceIt.

B. A PER SE RIGHT? ANONYMITY DECOUPLES FROM SPEECH

52. From these cases it would appear that a speech nexus is always required and that a right of anonymity only exists insofar as it has consequences for speech. But in fact, the Court has recognized a right to anonymity that is broader than simply political anonymity. In other words, even though the speech nexus will make a court's protection of anonymity more likely, such a nexus is not necessary in order to be protected by anonymity. Thus, courts have in general upheld juror anonymity[186], anonymity with respect to the abortion decision of a minor,[187] the anonymity of a rape victim in newspaper articles,[188] the anonymity of a pregnant student in a student newspaper,[189] the right to proceed anonymously in a court

---

[178] 364 U.S. 479 (1960).
[179] *Note: Anonymity: An Emerging Fundamental Right*, 36 IND. L.J. 306, 317 (1961).
[180] 240 F.3d 553 (6th Cir. 2001).
[181] *See, e.g.*, Doe v. 2TheMart.com Inc., 140 F.Supp. 2d 1088 (2001).
[182] *See, e.g.*, Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1607 (1999). "The Internet's… impact on the data processing model is a dramatic reduction of existing zones of data anonymity." *Id*. at 1644.
[183] *See, e.g.*, ACLU v. Miller, 977 F. Supp. 1228, 1230 (1997).
[184] "… cyberspace-enabled racial anonymity might prevent us from applying the rules of racial mapping." Jerry Kang, *Cyber-Race*, 113 HARV. L. REV. 1131, 1136 (2000).
[185] Donald Karl, *State Regulation of Anonymous Internet use after ACLU of Georgia v. Miller*, 30 ARIZ. ST. L.J. 513, 515 (1998).
[186] *See, e.g.,* United States v. Brown, 250 F.3d 907 (2001).
[187] *See, e.g*, Ohio v. Akron Ctr. for Reproductive Health, 497 U.S. 502 (1990).
[188] *See, e.g*, Florida Star v. B.J.F., 491 U.S. 524 (1989).
[189] *See, e.g*, Hazelwood Sch. Dist. V. Kuhlmeier, 484 U.S. 260 (1988).

action—even though a court is a public forum.[190] The interests protected by anonymity vary widely. "Anonymity is praised as a necessary component of free society on one hand, but condemned as a vehicle for nefarious activity on the other."[191] Still, the right to [anonymity] is a "quasi-right" that is protected in some instances but not in others.[192] Under this broader conception of anonymity, one might argue that FaceIt violates a *per se* right to anonymity because the program allows citizens in public places to be identified indiscriminately.

53. Another way to reformulate the value of anonymity is to argue that it encompasses a broader range of non-speech activities that nevertheless *implicate* speech. Under this conception, activities that are formative of identity (such as attending certain meetings, going into certain stores, viewing certain movies, and so on) are part of speech. Similarly, activities that help an individual formulate his or her thoughts—such as reading—are also closely tied to speech. These activities therefore should also be granted anonymity. Julie Cohen therefore argues for a right to *read* anonymously, because the activity of reading is as intimate and prior to the activity of speaking.[193] "Logically, that zone of protection should encompass the entire series of intellectual transactions through which they formed the opinions they ultimately chose to express. Any less protection would chill inquiry, and as a result, public discourse, concerning politically and socially controversial issues[…]."[194] One could argue that there is a right to be anonymous in public as well as it is expressive conduct. Attending a Green Party meeting or a Catholic mass requires walking in public and would almost certainly qualify as political and expressive conduct to which there might be a right to anonymity. But what about attending a New York Giants game—surely the expression implied is one's support for one of the teams—or a Yo Yo Ma concert? What about walking into the local McDonald's? No matter how trivial or incidental the expressive conduct, one could still argue that they have expressive value and should therefore be protected. The case for protection of anonymity is further bolstered by the fact that individuals appearing in public often do not have the option of hiding their faces under a mask, for instance. Court authority has been divided over whether or not ordinances prohibiting masks violate the First Amendment.[195] Usually, courts have held, however, that unless the masks themselves constituted symbolic speech (such as a KKK hood), ordinances preventing the wearing of masks that just hide identity are constitutional.[196] Once FaceIt is a

---

[190] *See, e.g*, Roe v. Aware Woman Ctr. for Choice, Inc., 253 F.3d 678 (2001).
[191] Shawn Helms, *Translating Privacy Values with Technology*, 7 B.U. J. SCI. & TECH. L. 288, 302 (2001).
[192] *Id*. at 306. *See, e.g.,* Privacy Act of 1974, 5 U.S.C. § 552a (1994 & Supp. V 2000); Cable Communications Policy Act of 1984, 47 U.S.C. § 551 (1994 & Supp. IV 1999); Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (1994); Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721 (1994); Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2703 (1994); McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342 (1995); NAACP v. Alabama ex rel. Patterson, 357 U.S. 449 (1958).
[193] Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at 'Copyright Management' in Cyberspace.* 28 CONN. L. REV. 981 (1996).
[194] *Id*. at 1007.
[195] Courts answered no in State v. Miller, 398 S.E.2d 547 (Ga.1990), and Schumann v. New York, 270 F. Supp. 730 (S.D.N.Y. 1967), for example, and yes in Ghafari v. Municipal Court, 87 Cal. App. 3d 255 (1978), and Aryan v. Mackey, 462 F. Supp. 90 (N.D. Tex. 1978), for example. *See also*, Church of the Am. KKK v. City of Erie, 99 F. Supp. 2d 583 (2000). In this case, an anti-mask ordinance was held to be unconstitutional as applied to members of the KKK because it prevented symbolic speech. In other regards it was held constitutional, however. Thus ordinary citizens, whose masks would not say anything symbolic but were designed simply to hide identity, would be legally prohibited under this ordinance.
[196] Am. KKK v. City of Goshen, 50 F. Supp. 2d 835 (1999).

common occurrence, ordinary citizens ought to have the right to protect their anonymity as well, either by wearing masks or by taking down the cameras. In any case, it is anonymity that might offer a vindication of rights and the privacy invasion that FaceIt carries itself.

VIII. CONCLUSION

54. Current biometric research has reached a point at which identification human beings can take place from a distance—without touching individuals, stopping them on the street. Research currently includes efforts to identify humans simply from the way they walk, or their gait.[197] Because of the rise of national databases that keep track of financial, health, sexual, consumer and other types of information, the danger to personal privacy comes from being able to link an individual to all these sources of information. FaceIt is different from other sense-enhancing technologies because it is almost used exclusively in a public sphere where it is able to sidestep the Fourth Amendment protection of the reasonable expectation privacy.

55. Under the current jurisprudence, it is not likely that the Fourth Amendment will protect citizens from technologies such as FaceIt. This article has argued that a re-conceptualization of the Fourth Amendment not so much as protecting individuals but more as demanding accountability and justification from the government as it does its searches might be necessary. Under this conception, a *de minimis* individualized suspicion would be required before FaceIt can scan an individual's face—this requirement might then essentially prohibit its indiscriminate use in public spheres. Anonymity might be another alternative because of its nexus to the public sphere and because FaceIt is a tool that is used to identify rather than to pry, so anonymity is a better fit than privacy.

56. With the rise of each new technology, courts strive to "carry forward established constitutional principles into the new context."[198] At the same time, however, the new technology strains the old principles and often requires "a new approach that has consequences for older technologies as well as the newer ones."[199] FaceIt is such a technology. It differs from the other technologies since the *Katz* decision in that it is used almost exclusively in public, but prominently so, and is able to identify even innocent parties from a distance without intrusion. The technology is by far the most "Orwellian", but at the same time the Fourth Amendment's expectation of privacy that traditionally has—with some difficulty—ruled out some technology is helpless against FaceIt. Only through a new conception of the Fourth Amendment that stresses the government's accountability and justification in conducting searches or a First Amendment protection of anonymity could this dystopia be postponed or even eliminated.

---

[197] DARPA projects include the funding of technology that can identify individuals based on their walk. Researchers have said that this technology is even better than face-recognition since it can perform identification from even farther away. "People have different styles of moving, due to their individual idiosyncrasies as well as the differences in physical dimensions and weights of body limbs. Because of these fundamental physical and behavioral differences, human motion provides a unique cue for identifying people at a distance." Carnegie Mellon University, DARPA ITO Sponsored Research, 2001 Project Summary *at* http://www.darpa.mil/ito/psum2001/k614-0.html.

[198] Paul Gewirtz, *Constitutional Law and New Technology*, Social Research v.64, Fall 1997, at 1191.

[199] *Id.*

57. Finally, it is to be noted that, courts are not the only institutional resort that privacy advocates have. Often technology such as FaceIt that citizens viscerally oppose will not be implemented because of popular sentiments. Examples illustrating this point abound: When, in the spring of 1990, the Lotus Corporation developed a database containing personal information about over 100 million households, was about to be launched, public outcry caused the company to withdraw the product.[200] In 1996, Yahoo was to launch its People Search service that provided addresses for 175 million people whose names were taken from commercial mailing lists. In response to the resulting outcry, Yahoo eliminated 85 million who had unlisted home addresses.[201] But it is important to realize that such opposition is only temporary, and that they are subject to the vicissitudes of national events. In the long run, it must be the courts that protect the individual even—especially—in the public sphere.

[200] *See, e.g*, M. CULNAN & H. SMITH,*'Lotus' Marketplace: Households-Managing Information Privacy Concerns*, COMPUTERS, ETHICS AND SOCIAL VALUES. (D. Johnson and H. Nissenbaum, eds. 1995).
[201] Ann Bartow, *Our Data, Ourselves: Privacy, Propertization, and Gender*, 34 U.S.F. L. REV. 633, 675 (2000).