NOTES

FACIAL RECOGNITION TECHNOLOGY, VIDEO SURVEILLANCE, AND PRIVACY

CHRISTOPHER S. MILLIGAN*

*"You are on a video camera an average of ten times a day. Are you dressed for it?"***

I. INTRODUCTION

A. BACKDROP TO THE FISHBOWL

1. *Orwellian Reflections*

> The telescreen received and transmitted simultaneously. Any sound that Winston made, above the level of a very low whisper, would be picked up by it; moreover, so long as he remained within the field of vision which the metal plaque commanded, he could be seen as well as heard. There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live—did live, from habit and instinct—in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.[1]

Of course, with night vision enhancement, Winston's movements could now be observed even in the black pitch of night. Today, the warnings of Orwell and others seem almost cliché. The United States is not the totalitarian society that Orwell envisioned. That Orwell's warnings do seem cliché perhaps means it is wise to be wary lest we become immune to intrusions on our privacy and personal autonomy.

---

* J.D. candidate, University of Southern California Law School, 2000. B.A., University of California, San Diego, 1996. The author would like to thank Professor Michael H. Shapiro for serving as his faculty advisor and the members of the Southern California Interdisciplinary Law Journal for their help in editing this Note. Thanks also to Eugenia Chiang for all of her help and support.

** Taken from an October 1998 Kenneth Cole advertisement in the Century City Shopping Mall, Los Angeles, California. A more appropriate question might be "Are you dressed at all?" Video surveillance has the ability to strip individuals of their privacy while making them feel naked before it.

[1] GEORGE ORWELL, 1984, at 6-7 (New American Library, Inc. 1961) (1949). Winston is the main character in the novel.

In the recent film The Truman Show, Jim Carrey portrays the hero of a modern saga being played out worldwide.[2] The unwitting, unknowing star of a popular television show, his entire life is controlled by a television producer and filmed through the use of surreptitious video surveillance.[3] The movie ends with Carrey's character leaving behind the blissful ignorance of his prior life and escaping from the studio set through a doorway painted into the edge of the sky.[4] In that moment he rejects those that would control and use him for their own purposes, while sedating him with the safety and comfort of the world they placed him in.

While this may all seem like a far cry from the visions depicted in George Orwell's *1984*[5] and Aldous Huxley's *Brave New World*,[6] the technologies featured within those novels are in existence today. Facial recognition technology, developed by the military for national security purposes, is already being used by private industry and by law enforcement agencies. This technology has the ability to instantly match an image with a name and the name with personal data. When used with digital video cameras, this technology can be used to scan, monitor and control access.

What is more, today there seem to be cameras everywhere. Everyone appears to be watching everyone else.[7] In Los Angeles' Bunker Hill neighborhood, for instance, almost every footfall is caught on tape. In *City of Quartz*, Mike Davis, while discussing the surveillance capabilities of the Los Angeles Police Department ("LAPD"), states that "[w]e are at the threshold of the universal electronic tagging of property and people—both criminal and non-criminal . . . monitored by both cellular and centralized surveillances."[8]

But there seems to be little, if any, debate about the creeping trend of technology and modern society to invade the individual's sphere of personal autonomy and privacy. This trend is often accepted as an

---

[2] THE TRUMAN SHOW (Paramount 1998). The concept that there is entertainment value in individuals' everyday activities is a common one in recent years. Other recent examples are the film EDTv (Universal 1999) and MTV's television series The Real World (1992-present), chronicling the lives of groups of young adults living together.

[3] *See* THE TRUMAN SHOW (Paramount 1998).

[4] *See id.*

[5] ORWELL, *supra* note 1.

[6] ALDOUS HUXLEY, BRAVE NEW WORLD (Harper & Row Publishers 1960) (1932).

[7] "[D]oesn't this creeping confluence of government snooping, commercial tracking and cultural tolerance of eavesdropping threaten each individual American's personal freedom?" William Safire, *Restore Some Privacy While You Still Can*, FT. LAUDERDALE SUN SENTINEL, Jan. 16, 1998, at 21A. *See also* Mark Hansen, *If Crime Is Everywhere, So, Too, May Be Police Surveillance Cameras and Contraband Detection Devices to Combat It. but Who's Looking Out for Privacy Rights?*, A.B.A. J., Aug. 1997, at 44, 47 (quoting John Henry Hingson III, a criminal defense lawyer in Oregon City, Oregon, "Technology has so numbed the American conscience and spirit, we don't even think about what it means for our way of life anymore . . . . It's like we've all been administered a massive dose of Novocain.").

[8] MIKE DAVIS, CITY OF QUARTZ 253 (1990).

inevitable result of modernization, technological change, globalization, and a shrinking world. It is also often accepted as a necessary evil to deal with an ever more dangerous world. Those who value privacy are laughed off as privacy freaks or dangerous kooks.[9] No one seems to be overly concerned and there is very little public discussion as we launch ourselves down this path.[10] There certainly is no well-organized lobby to protect citizens from video surveillance.[11] It is also doubtful whether the use of video surveillance in public places faces any significant constitutional obstacles.[12]

2. *Growth of the "Police State"*

Law enforcement is one of the fastest areas of federal government expansion in this era of downsizing and retraction of the federal welfare state.[13] The expansion of the police power of the federal government is occurring at the same time that many new, more sophisticated and powerful surveillance technologies are springing forth.[14] Not surprisingly, the prison industry has followed suit, as a leading growth industry in the United States.[15] The danger is that the growth of law enforcement will take on a life of its own.[16]

Much of the increase in police power due to advancement of surveillance technologies has arisen from the conversion of Cold War military technologies.[17] In 1994, Attorney General Janet Reno and Deputy Assistant Secretary of Defense John Deutch agreed to the joint development of advanced technologies and systems for use in both military and law enforcement operations.[18] The Central Intelligence Agency ("CIA") has worked with the Immigration and Naturalization Service

---

[9] A common response to those who voice privacy concerns is that if you don't do anything wrong, you needn't worry about surveillance. "Clearly the spread of surveillance has less to do with lawlessness than with order. 'Just don't do anything wrong,' advises the smiling cop monitoring the hidden cameras . . . 'and you have nothing to worry about.'" Mark Boal, *SpyCam City*, VILLAGE VOICE, Oct. 6, 1998, at 38.

[10] *See id.* ("With little public awareness and no debate, the scaffolding of mass surveillance is taking shape.").

[11] *See* Brock N. Meeks, *Privacy Lost, Anytime, Anywhere (Impact of Video Surveillance)*, COMM. ASS'N FOR COMPUTER MACHINERY, INC., Aug. 1, 1997, at 11, 11.

[12] *See* Hansen, *supra* note 7, at 45-46.

[13] *See* Peter Andreas, *The Rise of the American Crimefare State*, WORLD POL'Y J., Oct. 11, 1997, at 37, 37.

[14] *See id.*

[15] *See id.* at 38.

[16] *See id.* at 43.

[17] *See id.* at 41. *See also* Hansen, *supra* note 8, at 47 (quoting John Henry Hingson III, a criminal defense lawyer in Oregon City, Oregon, "The weapons of war are now being used against American citizens for civilian law enforcement . . . . And the casualties of this war are the constitutional rights of the innocent.").

[18] *See* Andreas, *supra* note 13, at 41.

("INS") to develop facial recognition technology, allowing individuals entering the United States to be identified by their facial structures.[19]

This cooperation mirrors the increased use of military agencies for law enforcement purposes (especially for the "war on drugs") and the federalization of law enforcement.[20] In 1981, Congress created exceptions to the Posse Comitatus Act, which prohibits military assistance in domestic law enforcement.[21] With the demise of the Cold War and the advent of the Drug War, the relationship between the federal military, intelligence structures and law enforcement has become quite intimate. The energies formally deployed towards Cold War national security objectives are now being arrayed for use in domestic policing and border maintenance.[22] In the process, this has led to the concern that growth in law enforcement will be self-perpetuating as military and intelligence institutions take refuge.[23]

It is obvious that the surveillance capacities of law enforcement agencies have undergone huge increases. In addition to the adoption of military technologies, there have been numerous advancements in civilian surveillance technologies of which law enforcement agencies have been able to take advantage. The Federal Bureau of Investigation's ("FBI") computers in the 1990s were nearly forty times as fast they were a decade before (this increase was ten times that of the Internal Revenue Service).[24] Data storage capabilities have increased in a similar exponential manner.

The growth in law enforcement seems all the more ironic and curious, given that actual crime rates are dropping and have been so for quite some time.[25] This calls into question the need to develop increased surveillance technologies in an era of supposed increased governmental austerity. However, public perception does not mirror the decrease in crime levels.[26]

Other questions arise from the fact that our current law is ill prepared to deal with the challenges presented by new surveillance technologies. After

---

[19] *See id.*

[20] *See id.*

[21] Congress passed the Posse Comitatus Act in response to the military presence in the South during the Reconstruction Era. Army Appropriations Act, ch. 263, § 15, 20 Stat. 145, 152 (1878) (codified as amended at 18 U.S.C. § 1385 (1994)). Congress created the exception to provide for military involvement in drug interdiction at United States borders. Department of Defense Authorization Act, 1982, Pub. L. No. 97-86, § 905, 95 Stat. 1099, 1114-16 (1981) (codified as amended at 10 U.S.C. §§ 371-80 (1994)). *See* Matthew C. Hammond, Note, *The Posse Comitatus Act: A Principle in Need of Renewal*, 75 WASH. U. L.Q. 953 (1997).

[22] *See* Andreas, *supra* note 13, at 41.

[23] *See id.* at 43.

[24] *See id.* at 39.

[25] *See, e.g.*, Roberto Suro, *Figures Show 7% Decline in Crime for 1998*, WASH. POST, May 17, 1999, at A5.

[26] *See* Patrick O'Driscoll, *Crime Rate Recedes, but Wariness Remains*, USA TODAY, Nov. 20, 1998, at 11A; Beth Shuster, *Statistics Say That Violent Crime is Declining, Yet Many Americans Still Feel Threatened. The Anxieties Are Stoked by Politicians, the Police, the Security Business and the Media. A look At Why We Are . . . Living in Fear*, L.A. TIMES, Aug. 23, 1998, at A1.

all, it took the Supreme Court some ninety years to apply the Fourth Amendment's protections for privacy to the telephone.[27] Professor Laurence Tribe of Harvard Law School has speculated that video cameras and other technological innovations may render traditional Fourth Amendment protections irrelevant.[28] Mass public monitoring through the use of video surveillance allows police to bypass court hearings and warrants.[29] Federal wiretap law places controls over the installation of electronic aural bugging devices in private dwellings, but no equivalent statutes address the similar placement of video surveillance.[30]

B. THESIS

The use of video surveillance and facial recognition for law enforcement and other purposes is an overly intrusive presence in individuals' lives. These types of surveillance technologies are inordinately intrusive into individual privacy to such an extent that they chill personal autonomy. For this reason, there should be specific legal protections (legislative *and* judicial) regulating these new technologies.

It is debatable, but unlikely, that under current law the use of video surveillance for law enforcement purposes would be found to be illegal or unconstitutional, even when used in conjunction with facial recognition technology. Several constitutional issues arise in regards to video surveillance and facial recognition technology. One issue is whether the use of facial recognition technology and video surveillance jointly constitute a search under the Fourth Amendment. A second issue is whether facial recognition software and video surveillance could be construed as unnecessarily chilling individuals' First Amendment freedoms of speech and association.

In addition to the constitutional issues, there are also social and ethical issues that merit public debate. These questions deal with whether people are willing to live their lives under the watchful lens of a camera and monitor—whether they are able to sacrifice personal autonomy and risk governmental abuse of their data for the sense of safety and order which video surveillance provides.

---

[27] *See* Boal, *supra* note 9, at 38. *See also* Hansen, *supra* note 7, at 47 (discussing *Katz v. United States*, 389 U.S. 347 (1967)). Prior to *Katz*, the Court generally held that only a search involving a physical trespass into a constitutionally protected area required a warrant.

[28] *See* Michael S. Serrill, *The No Man's Land of High Tech; New Devices Aid Police but Threaten the Right of Privacy*, TIME, Jan. 14, 1985, at 58, 58.

[29] *See* Boal, *supra* note 9, at 38. "Immediately after a crime, cops check cameras in the vicinity that may have captured the perp on tape." *Id.*

[30] *See* William C. Rempel, *Computer Age Gaps—Privacy Law: Race to Pace Technology*, L.A. TIMES, May 14, 1985, at A1.

C. STRUCTURE OF THIS NOTE

Part II discusses the technology behind and uses for video surveillance (closed circuit television ("CCTV")).[31] Part III discusses the emerging technologies that drive facial recognition applications, their use in conjunction with video surveillance, and other uses. Part IV reviews other new surveillance technologies, including other biometric identification and scanning devices, and describes the relative superiority of facial recognition technology. This section also discusses the different ways in which these technologies can be implemented, such as national identification cards. Part V explores the meaning of privacy, privacy rights, and their applicability to facial recognition technology, video surveillance, and other emerging surveillance technologies. In so doing, Part V analyzes the legal and statutory development of privacy rights to surmise whether video surveillance incorporating facial recognition technology is incompatible with judicial and legislative history. Part VI outlines arguments both in favor and against the legality and morality of using facial recognition technology and video surveillance. Part VII concludes that facial recognition software and video surveillance can be used in ways that violate personal autonomy and a person's reasonable expectation of privacy. It then discusses possible judicial and legislative responses. Finally, this Note offers several views on what the future holds for privacy rights and personal autonomy in light of recent advances in the field of surveillance technology.

II. VIDEO SURVEILLANCE AND CLOSED CIRCUIT TELEVISION

A. HISTORICALLY

1. *United Kingdom and Abroad*

Video surveillance has long been a way of life in much of Europe.[32] In the United Kingdom, CCTV and video surveillance is used on an enormous scale—currently over seventy-five cities are using it to monitor urban centers and approximately ninety-five percent of all local governments are considering using it as a law enforcement measure.[33] Interestingly, Great

---

[31] Video surveillance is normally conducted through CCTV systems. A CCTV system can be as simple as a single camera, monitor and a recorder.

[32] *See* Hansen, *supra* note 7, at 45.

[33] *See* Quentin Burrows, *Scowl Because You're on Candid Camera: Privacy and Video Surveillance*, 31 VAL. U. L. REV. 1079, 1099 (1997). "[I]n England, the government has spent more than $30 million, installing thousands of street corner surveillance cameras, and those cameras are credited with a 13.4 percent drop in regional crime." Janet Ward, *Beyond the Big Brother Syndrome*, AM. CITY & COUNTY, Oct. 1998, at S4, S6 (Supp.).

Britain has not implemented any substantive legal protections or regulation of video surveillance use.[34]

Elsewhere, the list of nations that use video surveillance in public places for law enforcement purposes includes France, Australia, Ireland, and Scotland.[35] Cities in Europe that have installed video surveillance cameras have claimed dramatic reductions in crime rates.[36]

2. *United States*

Over sixty urban centers in the United States use video surveillance in public places for law enforcement purposes.[37] Tacoma, Washington, is believed to be the first city in the country to publicly announce that they use video surveillance for law enforcement purposes.[38] However, Baltimore, Maryland, has what is considered the most expansive video surveillance system in place in the United States, and the city is considering expanding it.[39]

Television broadcasting and viewers in the United States seem addicted to the vicarious thrill of watching invasions of others' privacy. There is an abundance of "real life" television programs that make use of video surveillance and CCTV programming—*COPS* and *Rescue 911*, among others.[40] Investigative news programs like *60 Minutes* make use of hidden cameras, while local network affiliates replay footage from police and liquor store video cameras on their nightly news broadcasts.[41] Apparently broadcasters will continue to have plenty of footage to use, as the use of CCTV systems will undoubtedly continue to increase.[42]

---

[34] *See* Burrows, *supra* note 33, at 1099.

[35] *See id.* at 1101-02.

[36] *See id.* at 1123. In Newcastle, England where one of the first CCTV systems was introduced in 1992, research showed an 11% decline in assaults, a 49% drop in burglary, and a 44% drop in criminal damage from the end of 1991 through the end of 1994. *See* John Deane, *CCTV Boost Follows Crime-Fighting Success*, PRESS ASS'N NEWSFILE, Oct. 13, 1995, *available in* LEXIS, News Library, Arcnws File.

[37] *See* Boal, *supra* note 9, at 38.

[38] *See* Hansen, *supra* note 7, at 45.

[39] *See id.*

[40] *See* Burrows, *supra* note 33, at 1107.

[41] *See id.* at 1108.

[42] *See* Tina D'Aversa-Williams, *Industry Outlook: An Active Six Months for M&As*, ACCESS CONTROL & SECURITY SYSTEMS INTEGRATION, July 30, 1998, *available in* 1998 WL 9308190. The greatest growth area among all security products through the millennium will be closed circuit television systems. *See id.*

B. USES

1. *Law Enforcement and Crime Prevention*

Law enforcement agencies have used video surveillance both as a method to apprehend criminals after the fact and as a means of crime prevention. These agencies also use clandestine video surveillance to build cases against criminal suspects. Police use both police operated camera systems (in those areas where they exist) and privately operated surveillance systems to identify those who engage in criminal activity.[43]

Police in a number of cities utilize video and camera surveillance to prevent traffic violations and catch scofflaws.[44] In Los Angeles, California, cameras are positioned at certain street intersections to enforce stoplights by capturing license plate images.[45] Those drivers who run a red light can expect to receive a citation in the mail.[46] Elsewhere, the same mechanism enables video and camera surveillance to enforce speed limits.[47] In Scotland, there are an estimated 10,000 cameras in place monitoring traffic, speed, and parking structures.[48]

2. *Other Uses*

Besides law enforcement, video surveillance has been used for a variety of other purposes. A large number of companies and businesses use hidden cameras to monitor employee productivity, to deter theft and fraud, or to ensure safety in the workplace.[49] Retailers have used video surveillance in their loss-prevention programs for a number of years. And anyone who is a fan of spy literature or films is familiar with the ways in which video and camera surveillance has been used for purposes of espionage—foreign, domestic, and industrial.

Voyeurism and perversions drive many applications of video surveillance technology.

> The harvest from hidden cameras can also end up on the Internet, via the many Web sites that offer pics of women caught unaware. There are hidden toilet cams, gynocams, and even the intrepid dildocam . . . . Their

---

[43] *See* David R. Baker, *Security Cameras Have Eye on You; Lost Privacy Cost of Safety*, L.A. DAILY NEWS, May 24, 1998, at N1. "So common are surveillance cameras in stores that police routinely check their videotapes near crime scenes, hoping the electronic eyes have spied something useful." *Id.*

[44] *See* Burrows, *supra* note 33, at 1083. In Fairfax, Virginia, an intersection surveillance system has been credited for causing a drop in red light violations. *See* Ward, *supra* note 33, at S6.

[45] For example, in Los Angeles, California, surveillance cameras patrol La Cienega Boulevard at three different intersections: Sunset Boulevard, Melrose Avenue, and Wilshire Boulevard.

[45] *See* Burrows, *supra* note 33, at 1083 & n.42.

[47] *See id.*

[48] *See* Alastair Dalton, *Controls Urged on Big Brother's All-Seeing Eyes*, SCOTSMAN, July 23, 1998, at 9.

[49] *See* Boal, *supra* note 9, at 38.

popularity suggests that whatever the rationale, surveillance cameras resonate with our desire to gaze and be gazed upon.[50]

C. RECENT TECHNOLOGICAL ADVANCES

1. *Digitization*

Video surveillance technology was first introduced in 1956.[51] Video surveillance and closed circuit television systems have been the subject of a number of technological advancements in recent years. The digitization of images caught on video allows for the easy and inexpensive reproduction and transferability of video images. It also allows the digital data representing these images to be easily stored for an indefinite period of time.[52]

2. *Miniaturization*

The miniaturization of video surveillance equipment and the diminishing cost of this technology have allowed law enforcement and private consumers to increase their use of video surveillance.[53] The technology can now be operated more clandestinely and unobtrusively, and can be placed in areas where it previously was not possible.[54] Because of the low cost and clandestine nature of present video surveillance technology, users often supplement visible, obtrusive camera systems with hidden, unobtrusive cameras.[55] Pinhole video cameras are now available that fit in the palm of one's hand and can be hidden almost anywhere.[56]

---

[50] *Id.*

[51] *See* Burrows, *supra* note 33, at 1080.

[52] *See* FRED H. CATE, PRIVACY IN THE INFORMATION AGE 16 (1997).

> [W]e are witnessing an explosion in digital data, which is dramatically raising the costs of failing to address the issues that new information technologies pose. As every facet of society relies more heavily on electronic information technologies and data, the ramifications of no solutions or poor solutions to those issues become more significant. The more heavily U.S. businesses invest in . . . [these] technologies, and the more expectations as to the legal framework in which those systems operate are solidified, the more difficult and costly it will be to change behaviors.

Id.

[53] *See* Boal, *supra* note 10, at 38. "Today, a pinhole camera lens can be the diameter of less than one eighth of an inch." Burrows, *supra* note 34, at 1080.

[54] *See* Boal, *supra* note 9, at 38.

[55] *See id.*

[56] *See* Burrows, *supra* note 33, at 1080.

III. FACIAL RECOGNITION TECHNOLOGY

A. EMERGING TECHNOLOGY

"A hundred bucks at a computer store already buys face-recognition software that was classified six years ago . . . ."[57] As a system of identification, it is relatively unobtrusive and non-invasive, especially when compared with other biometric identification systems. A number of corporations have designed software applications for the technology.[58] Visionics Corporation recently received an award from the United States Department of Defense for its software applications.[59] The application searches for matches from a watch-list, a video library of known individuals, stored in a law enforcement database.[60] It is capable of offering a percentage score based on how confident the system is of a correct identification.[61] Faces that do not match those in the database are immediately discarded.[62] Software applications from other manufacturers work in a similar fashion.

The software uses algorithms to recognize and then represent patterns and relationships in human facial features.[63] This is similar to the way in which the human brain recognizes and remembers facial images.[64] It can locate and identify human faces from live video or static images, at angles of up to thirty-five degrees, while compensating for lighting conditions, skin color, eyeglasses, facial expressions, facial hair, and aging.[65] The software is then capable of building a time stamped database of facial images for storage, later analysis, and comparisons.[66]

Another application is aptly termed Facematcher.[67] Designed by a California software company, it goes through a database of facial images at a thousand images per minute, making it unnecessary, for example, for an individual to go through a number of police mugshot books.[68]

---

[57] Boal, *supra* note 9, at 38.

[58] *See* Ken Phillips, *Face Recognition Gears Up*, P.C. WEEK, Oct. 27, 1997, at 108, 108.

[59] *See Visionics and Ultrak Announce Partnering Agreement; Ultrak Will Now Offer Visionics' Leading Face Verification Technology in Its SAFEnet High-End Access Control System*, May 28, 1998, *available in* 1998 WL Business Wire, Press Release Wires.

[60] *See Find Criminals, Missing Children, Even Terrorists in a Crowd Using Face Recognition Software Linked to a Database*, Nov. 16, 1998, *available in* 1998 WL Press Release Newswire, Press Release Wire [hereinafter *Find Criminals*].

[61] *See id.*

[62] *See id.*

[63] *See id.*

[64] *See id.*

[65] *See id.*

[66] *See id.*

[67] *See* Steve Carney, *Computer Puts Names to Faces of Criminals*, L.A. TIMES, Oct. 27, 1997, at B1.

[68] *See id.*

The appeal and power of Facematcher come from its ability to operate on any standard 233 megahertz Pentium powered desktop computer (no need for access to a government supercomputer).[69] Like the software from Visionics corporation, it does not give 100% probability, but instead lists the highest probabilities.[70] The application lays a grid over the facial image and measures the distance between facial features; distances and angles of facial features are compared by computer and potential images.[71] Images from any source, such as a high school yearbook, driver's license, or passport photos, could be stored in application databases for later comparison.[72]

B. INTEGRATION WITH OTHER BIOMETRIC APPLICATIONS

Facial recognition technology can easily be used in combination with other biometric information, such as fingerprint or retinal scanning.[73] Biometric data can also be correlated with personal information of any kind—an individual's medical history, tax records, criminal arrest records, voting records, political affiliations, and any other conceivable type of information.[74] Already, there are even plans among some companies to marry biometric data from facial recognition systems with data gleaned from supermarket checkout counters.[75]

Many companies that make security access cards now also offer CCTV and biometric systems.[76] As well, partnerships among companies offering complementary surveillance and security technologies are on the rise.[77]

C. USES

There are two main uses for facial recognition technology: first, for identification purposes, and second, for access control or authorization purposes.[78]

---

[69] *See id.*
[70] *See id.*
[71] *See id.*
[72] *See id.*
[73] *Cf.* John D. Woodward, *Biometric Scanning, Law & Policy: Identifying the Concerns—Drafting the Biometric Blueprint*, 59 U. PITT. L. REV. 97, 140 (1997) ("[G]iven the various government agencies involved in evaluating biometric technologies and their many applications, there will likely not be a single dominant technology that emerges. Rather, biometric balkanization will take place . . . multiple technologies will be deployed . . . .")
[74] *Cf.* David A. Petti, *An Argument for the Implementation of a Biometric Authentication System ("BAS")*, 80 J. PAT. & TRADEMARK OFF. SOC'Y 703, 728 (1998) (describing privacy groups' fears of a national databank composed of the biometric signatures used by ordinary people in their daily commercial and private transactions).
[75] *See* Meeks, *supra* note 11, at 11.
[76] *See* D'Aversa-Williams, *supra* note 42.
[77] *See id.*
[78] *See* Woodward, *supra* note 73, at 100.

1. *Identification*

Identification is the ability to identify one person from among all those whose biometric identifying patterns have been recorded.[79] Law enforcement agencies are able to use facial recognition software to identify criminals and criminal activity after a crime has occurred by taking video surveillance images and using facial recognition software to identify perpetrators.[80] In like manner, they can identify known criminals or other undesirables through active scanning of facial images with simultaneous comparison to a database of compiled facial images.[81] As previously mentioned, such a database could include high school yearbook photos or driver's license pictures.[82]

This ability to simultaneously scan facial images and compare those images with others already entered and indexed into a database would give officials the ability to immediately identify known drug smugglers at border crossings, fugitives from justice at internal checkpoints, terrorists at airports, or even violent hooligans at soccer games.[83]

2. *Authentication*

Authentication is the ability to verify a person's identity through a comparison with their previously recorded biometric measurements.[84] Facial recognition technology has proved useful to control access and verify authorization in a number of different areas.[85] Government agencies can use it to prevent fraud in welfare and other entitlement programs.[86] A state's Department of Motor Vehicles ("DMV") could use the technology to scan databases to insure that individuals attempting to get a driver's license are who they say they are.[87]

Private industry can also use the technology to prevent fraud and loss. Many companies are currently searching for a way to convince consumers that they can engage in commerce over the internet ("e-commerce") with confidence that their credit or personal identity information will not be stolen.[88] Financial institutions are looking for ways to incorporate biometric data, such as facial recognition technology, into their methods of

---

[79] *See id.*
[80] *See* Carney, *supra* note 67, at B1.
[81] *See id.*
[82] *See id.*
[83] *See* Richard Thomas, *As UK Crime Outstrips US, A Hidden Eye Is Watching*, OBSERVER, Oct. 11, 1998, *available in* 1998 WL 18713569.
[84] *See* Woodward, *supra* note 73, at 100.
[85] *See* Phillips, *supra* note 58, at 108.
[86] *See* Woodward, *supra* note 73, at 140.
[87] *See id.*
[88] *See id. See also* Petti, *supra* note 74, at 711.

authorization for wire transfers, check cashing, and automatic teller machine access.[89]

Biometric facial scanning can also be used to control access at sensitive security checkpoints, such as for entrance to secure buildings and for computer and network log-on access.[90] Similarly, facial recognition can be used in residential areas to restrict access to residents.[91]

D. PRIVACY CONCERNS

The ability to instantly identify individuals by their facial features and access corresponding data leads to a number of concerns about possible misuse of data and privacy invasion. Such a system could be used to monitor and affect human behavior on an enormous scale.

IV. OTHER NEW SURVEILLANCE TECHNOLOGIES

A. OTHER BIOMETRIC IDENTIFICATION AND SCANNING DEVICES

The number of new biometric technologies currently coming on-line is impressive, to say the least. The market for biometric technologies is expected to grow from sixteen million dollars in 1996 to between fifty and one-hundred million dollars in 1999.[92] Fingerprint identification, the old standard, has quietly been improved, supplanted and supplemented. These new technologies use algorithms to compare measurements of individuals' hand features.[93] Technology is also available that allows individuals to be compared based on the vein patterns formed on the back of their hands.[94]

1. *Voice Recognition*

Voice recognition technology takes the acoustic signature of a person's voice and digitally converts and stores it.[95] Chase Manhattan Bank currently uses the technology to verify account access over the telephone.[96] The drawbacks to voice recognition are that individuals' voices can change and recording a vocal signature requires large amounts of computer memory.[97]

---

[89] *See id.* at 712-14.
[90] *See* Woodward, *supra* note 73, at 111.
[91] *Cf.* Woodward, *supra* note 73, at 111.
[92] *See id.* at 109.
[93] *See id.* at 104.
[94] *See id.* at 108.
[95] *See id.* at 107.
[96] *See id.*
[97] *See id.*

2. *Signature Recognition*

Signature authentication digitally records the style, pressure, speed, and other characteristics of an individual's signature.[98] Retail stores like Home Depot use signature recognition devices as a fraud reduction measure.[99] The disadvantage of using signature recognition systems is that they are not very reliable long-term.[100]

3. *Fingerprint Imaging*

Fingerprint imaging, the descendant of fingerprint identification, requires the individual to place a finger on an optical scanner which scans and then digitally records the fingerprint's signature.[101] Woolworth's supermarkets in Australia currently use fingerprint imaging to monitor employee attendance.[102] While fingerprint imaging enjoys a wide acceptance by the public, it is somewhat intrusive due to the need for physical contact with the scanner.[103]

4. *Hand Measurement Scans*

Hand geometrics make a three-dimensional record of hand and finger measurements.[104] The hand is placed on an optical scanner and a digital map is recorded.[105] Hand measurement scans are currently used by Walt Disney World in Orlando, Florida, to deter fraudulent use of annual passes.[106] Its main disadvantage is that hand measurements are relatively non-unique.[107]

5. *Hand Vein Mapping*

Hand vein mapping measures the pattern of veins on the back of an individual's hand.[108] Hand veins are not easily damaged and do not change over a lifetime.[109] However, vein mapping is somewhat intrusive, as it also requires, like finger imaging,[110] for the hand to be in close proximity to the mapping device.

---

[98] *See id.*
[99] *See id.*
[100] *See id.*
[101] *See id.* at 104.
[102] *See id.* at 105.
[103] *See id.*
[104] *See id.*
[105] *See id.*
[106] *See id.* at 106.
[107] *See id.*
[108] *See id.* at 108.
[109] *See id.*
[110] *See id.* at 105.

6. *Iris Recognition*

Iris recognition scans the structure of the iris using standard video technology, usually from a short distance away.[111] This technology captures the information and stores it digitally.[112] Its disadvantages are that it is somewhat intrusive and requires large amounts of computer memory storage.[113]

7. *Retinal Scans*

Retinal scanning involves a survey of the blood vessels of the retina using an incandescent light.[114] The image is then mapped and digitally stored in a database.[115] Retinal scanning relies on the fact that every individual's retina is unique and changes very little over the course of a lifetime.[116] The main disadvantage of the retinal scan is its relative intrusiveness, as it requires the individual to be in close proximity to the scanning device.[117]

B. CONTINUING FEDERAL BIOMETRICS RESEARCH EFFORTS

The federal government has established an organization, the Biometrics Consortium (founded by the National Security Agency), to head research, development, and applications of biometric technology.[118] The Biometric Consortium addresses ethical and legal issues surrounding the technology's use while also helping government agencies select and implement applications of biometrics.[119]

C. OTHER NEW SURVEILLANCE TECHNOLOGIES

1. *Aerial Thermal Imaging*

Originally developed by the military to locate enemy forces during combat, the Forward Looking Infrared Device ("FLIR") detects infrared heat emissions.[120] Infrared light passes through a lens and is received by a detector, which converts the thermal energy into a color and displays the

---

[111] *See id.* at 104.
[112] *See id.*
[113] *See id.*
[114] *See id.* at 103.
[115] *See id.*
[116] *See id.*
[117] *See id.*
[118] *See* Joseph P. Campbell, Jr. & Lisa Alyea, *Update on the US Government's Biometric Consortium* (visited Nov. 6, 1999) <http://www.biometrics.org/REPORTS/CTST95.html> (cited in Woodward, *supra* note 73, at 147).
[119] *See* Woodward, *supra* note 73, at 147.
[120] *See* Scott J. Smith, *Thermal Surveillance and the Extraordinary Device Exception: Re-defining the Scope of the Katz Analysis*, 30 VAL. U. L. REV. 1071, 1079 (1996).

color variations on a screen.[121] The technology is available both in the form of a small handheld detector and as a more advanced model that is attached underneath helicopters.[122] It is capable of detecting human activity and heat-emitting devices throughout buildings and homes.[123]

2. *Back-Scattered X-Ray Imaging*

In a Los Angeles federal courthouse, a device using back-scattered x-ray imaging is currently being tested.[124] The technology is used to develop a digitally enhanced sketched outline of an individual's body as well as anything that is being carried on their person.[125] The technology can potentially be used at a number of sites where access control is considered important, such as airports, prisons, and border crossings.[126]

3. *Passive Millimeter Wave Imaging*

Similar to back-scattered x-ray imaging, passive millimeter wave imaging can also be used to see through an individual's clothing to detect weapons and other items.[127] Its advantage over back-scattered x-ray imaging is that the device is mobile and can be used to scan individuals from some distance.[128]

4. *Radar Skin Scanning*

The radar skin scanner is an even more accurate way of scanning an individual's body and discerning any weapons carried.[129] It is capable of revealing anatomical details and, apparently, can even disclose whether a man has been circumcised.[130]

D. NATIONAL IDENTIFICATION CARDS

Any of the above biometric applications, as well as facial recognition technology, can be used in combination with card access systems to better control access or authorization.[131] Likewise, they can be used in

---

[121] *See id.*

[122] *See id.* at 1080.

[123] *See id.* at 1081-83. "More shocking, however, is the training literature which . . . . required operators to determine the precise amount of coffee in a cup and to identify the tear ducts on a human face." *Id.* at 1082-83.

[124] *See* Hansen, *supra* note 7, at 46.

[125] *See id.*

[126] *See id.*

[127] *See id.*

[128] *See id.*

[129] *See id.*

[130] *See id.*

[131] *See generally Applications,* ACCESS CONTROL & SECURITY SYSTEMS INTEGRATIONS, Apr. 30, 1998, *available in* 1998 WL 9308072 (discussing the use of card access systems for surveillance at border crossings, and in college classrooms and business buildings).

combination with identification cards.[132] Many states are experimenting with adding biometric signatures to driver's licenses.[133]

E. SUPERIORITY OF FACIAL RECOGNITION TECHNOLOGY

Presently, no biometric technology either has a perfect record or is foolproof.[134] However, facial recognition technology has certain benefits that others lack.[135] For authorization purposes, it is the least obtrusive and invasive of all the biometric technologies.[136] For law enforcement and identification purposes, it is equally effective by allowing for quick scanning of large numbers of persons from a safe distance and without the subject's knowledge.[137] Many of the other biometric technologies require the subject to be in very close proximity to the scanning device.[138] Presently, the major drawback is that the video camera angle does not always afford enough exposure for the software to identify patterns in the facial features.[139] However, this problem can be mastered through the use of additional cameras and will likely be greatly overcome as the technology improves.

V. PRIVACY

A. HISTORY IN THE UNITED STATES

Supreme Court Justice Louis Brandeis once identified the right to privacy, or as he termed it—"the right to be let alone," as one of the necessities for the enjoyment of life.[140] He also warned that new technologies could threaten this.[141] But the high regard with which privacy has been held in this country has always been juxtaposed with "a desire to regulate moral life, a suspicion of secrecy, [and] a democratic impulse to openness."[142] Our respect for privacy derives its roots partially from the

---

[132] *See generally* Woodward, *supra* note 73, at 113 (discussing the use of iris recognition technology and identification cards in verification systems).

[133] *See id.* at 110-11.

[134] *See id.* at 102.

[135] *See* Gayle Bryant, *Big Brother Is Watching, and He Knows Your Face*, BUS. REV. WKLY., July 27, 1998, at 110, 110. *See also* Woodward, *supra* note 73, at 106 (describing the advantages and reported disadvantages of facial recognition technology).

[136] *See* Bryant, *supra* note 135, at 110.

[137] *See Find Criminals*, *supra* note 60.

[138] *See* Woodward, *supra* note 73, at 102-07.

[139] *See* Thomas, *supra* note 83.

[140] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

[141] *See id.* at 195; *see also* Burrows, *supra* note 33, at 1085 ("Brandeis [was] concerned with the new technological invasions of the camera, the printing press, tabloid papers, and the telephone.").

[142] Miriam Horn, *Shifting Lines of Privacy: Today's Anxieties Mirror Earlier Debates in America's History*, U.S. NEWS & WORLD REP., Oct. 26, 1998, at 57, 57.

political writings of John Locke and Thomas Hobbes, which is reflected in our liberal democratic form of government.[143]

In the seventeenth century, there was not a well-developed concept of privacy in the American colonies.[144] Living quarters were often small and cramped, making it difficult to maintain privacy.[145] In puritan New England, neighborly spying was often seen as a civic obligation, necessary to an orderly society.[146] Adultery was a crime punishable by death, at least for women.[147] A gradual distinction between public and private began to emerge during the eighteenth century, as the United States became more cosmopolitan.[148] Living quarters were built with more space and with separate rooms and walls,[149] and the Constitution protected those homes from search and seizure, and the quartering of troops.[150]

Journalistic invasions of the privacy of public figures became a common occurrence during the nineteenth century.[151] With the advent of quick photography and mass-circulation newspapers, the latter part of the century saw the first invasion of privacy lawsuits in the United States.[152] Freud's writings in the early twentieth century advocated that the inner workings of the psyche are best unearthed and exposed.[153] During the Cold War, the McCarthy era saw stepped up government surveillance of individuals in the name of national security; essentially private matters, such as sexual orientation and membership in "subversive" political organizations, were the basis for accusations of treason.[154] Ironically, while suburbia and the automobile increased personal autonomy and the daily anonymity of life, Cold War tensions made it increasingly necessary to find out what our neighbors were doing.[155]

---

[143] *See* PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 43 (1995). "Although clearly privacy is important as part of this liberal tradition, its manifestation throughout American history is complicated both by difficulties in conceptualizing it and by technological and cultural changes that have affected the meaning of privacy and the ability to achieve privacy." *Id.*

[144] *See* Horn, *supra* note 142, at 59.

[145] *See id.*

[146] *See id.*

[147] *See id.*

[148] *See id.*

[149] *See id.*

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

[151] *See* Horn, *supra* note 142, at 57.

[152] *See id.* The first invasion of privacy case to reach an appellate court in the wake of the *The Right to Privacy*, Warren & Brandeis, *supra* note 140, involved image appropriation. *See* Andrew Jay McClurg, *Bringing Privacy Law Out of the Closet: A Tort Theory of Liability for Intrusions in Public Places*, 73 N.C. L. REV. 989, 1004 (1995) (discussing *Robertson v. Rochester Folding Box Co.*, 64 N.E. 422, 422 (1902)).

[153] *See* Horn, *supra* note 142, at 57.

[154] *See id.* at 58.

[155] *See id.*

Today, battles over privacy reflect historical conflicts.[156] There is always tension between the individual need for privacy and autonomy, and the sense that society suffers when morality goes unregulated.[157] Of course, society is also thought to suffer from excessive public exposure of private impulses.[158] Television and the video camera erase the lines between the public and private, allowing private lives to be put on public display.[159]

B. LEGAL UNDERPINNINGS: JUDICIAL AND LEGISLATIVE HISTORY

There is no specific constitutional right to privacy. However, the Supreme Court has developed a limited right of privacy based on a jurisprudence of fundamental rights in a string of cases—*Griswold v. Connecticut*,[160] *Roe v. Wade*,[161] *Whalen v. Roe*,[162] and *Bowers v. Hardwick*.[163] The Supreme Court has described this right as a "penumbral right," flowing from the emanations of the First,[164] Third,[165] Fourth,[166] Fifth,[167] Ninth,[168] and Fourteenth[169] Amendments.[170] It generally has been limited to certain rights of privacy and autonomy in individuals' intimate life decisions, such as

---

[156] *See id.*
[157] *See id.*
[158] *See id.*
[159] *See id.*
[160] 381 U.S. 479 (1965).
[161] 410 U.S. 113 (1973).
[162] 429 U.S. 589 (1977).
[163] 478 U.S. 186 (1986).
[164] The First Amendment states: "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press, or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." U.S. CONST. amend. I.
[165] The Third Amendment states: "No soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law." U.S. CONST. amend. III.
[166] The Fourth Amendment states:

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

U.S. CONST. amend. IV.
[167] The Fifth Amendment states: "No person shall . . . be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law . . . ." U.S. CONST. amend. V.
[168] The Ninth Amendment states: "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people." U.S. CONST. amend. IX.
[169] The Fourteenth Amendment states:

> No state shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.

U.S. CONST. amend. XIV, § 1.
[170] *See* Burrows, *supra* note 33, at 1090-91 (discussing *Griswold v. Connecticut*, 381 U.S. 479, 484-85 (1965)).

whether to have children or to engage in consensual sexual intercourse while married.[171]

1. *Criminal Procedure, the Fourth Amendment, and Wiretapping*

The placement of surveillance devices on a subject's private property by law enforcement agencies requires a "search" warrant issued by a court.[172] Courts have generally expressed a willingness to approve both audio and video surveillance provided that the type of crime necessitates it and the surveillance does not involve the observance of purely private activities. Courts have not yet been presented with the question of the use of facial recognition technology in connection with video surveillance.

Olmstead v. United States was the first instance in which the Supreme Court addressed audio surveillance.[173] In *Olmstead*, federal prohibition officers intercepted telephone conversations that led to the defendants' arrest for the unlawful possession, transportation, importation, and sale of intoxicating liquors.[174] The Court held that wire-tapping and listening to private telephone conversations did not properly constitute a "search" under the Fourth Amendment.[175] The Court felt that the Fourth Amendment only addressed physical intrusions and not the electronic interception of telephone conversations.[176]

The Supreme Court subsequently overruled *Olmstead* in *Katz v. United States*.[177] In *Katz*, the government intercepted the defendant's conversation as he was talking in a public telephone booth by attaching a listening device to an exterior panel of the booth.[178] The parties' arguments focused on whether a telephone booth was a protected area for purposes of the Fourth Amendment.[179] Finding that there had been a violation of the Fourth Amendment, the Court rejected the traditional approach used in *Olmstead* which defined a "search" as a physical trespass into a traditionally

---

[171] *Cf. id.* at 1091-93. "In *Griswold v. Connecticut*, the court changed the field of privacy . . . . spark[ing] a new type of privacy that resulted from a combination of technological advances in birth control and the personal choice to exercise privacy rights in this area." *Id.* at 1091 (discussing *Griswold*, 381 U.S. 479 (1965)).

[172] *See* Chip Johnson, *Techno-Cops: Police Tools of the '90s Are Highly Advanced, but Privacy Laws Lag*, WALL ST. J., Nov. 12, 1990, at A1.

[173] 277 U.S. 438 (1928).

[174] *See id.* at 455.

[175] *See id.* at 466.

[176] *See id. See also* Denise Troy, Comment, *Video Surveillance—Big Brother May Be Watching You*, 21 ARIZ. ST. L.J. 445 (1989) (surveying how federal courts treat video surveillance in the absence of express legislation, and highlighting the principles of Title III covering audio surveillance that federal courts have borrowed).

[177] 389 U.S. 347, 353 (1967).

[178] *See id.* at 348.

[179] *See* William O'Callaghan, *Cameras in the Restroom: Police Surveillance and the Fourth Amendment*, 22 HASTINGS CONST. L.Q. 867, 871 (1995).

protected area.[180] Instead, the Court believed that the Fourth Amendment should protect all that a person actively seeks to keep private.[181] Information that is knowingly exposed to the public is not entitled to such protection.[182] Or as Justice Harlan interpreted the majority opinion—a warrantless search where a person has a reasonable expectation of privacy violates the Fourth Amendment.[183] According to Justice Harlan, the Court used a two part test; first, the person must have a subjective expectation of privacy, and second, society must objectively recognize this privacy interest.[184]

Federal courts have borrowed the standards handed down by the Supreme Court in audio surveillance cases to apply when reviewing the legitimacy of video surveillance orders.[185] In *United States v. Torres*, the Seventh Circuit upheld the use of video surveillance, balancing the necessity of the surveillance against the level of intrusion (the type of crime involved weighed against the premises where the video surveillance was used).[186] The government had obtained an order allowing video surveillance to be placed in a "safe house" of an organization suspected of terrorist activities.[187] The court concluded that the order allowing the video

---

[180] *See Katz*, 389 U.S. at 353. Thus, the fact that the electronic device used did not penetrate the wall of the phone booth was of no constitutional significance. *See id.* at 352-53.

[181] *See id.* at 352.

[182] *See id.* at 361. *See also* Smith, *supra* note 120, at 1091-92 (discussing Justice Harlan's concurring opinion which has emerged as the foundation for the *Katz* formula as it exists today).

[183] *See Katz*, 389 U.S. at 363. The subjective prong of the majority's test has often been criticized. Joshua Dressler explains the criticism as follows:

> [I]f the subjective component is taken seriously, the government can eliminate privacy expectations by the simple act of announcing its intention to conduct Orwellian surveillance. Once people know that the government is reading their mail, listening to their conversations, and generally intruding on their privacy, they will have no subjective expectation of privacy.

JOSHUA DRESSLER, UNDERSTANDING CRIMINAL PROCEDURE, § 30(D)(2) (1991). However, the subjective prong has not been rejected by a majority opinion of the Court. *See* O'Callaghan, *supra* note 180, at 873.

[184] *See Katz*, 389 U.S. at 361.

[185] *See* 751 F.2d 875, 880-81 (7th Cir. 1984). To date, federal appellate courts have decided only three cases involving video surveillance. *See id.* at 875; United States v. Biasucci, 786 F.2d 504 (2d Cir. 1986); United States v. Cuevas-Sanchez, 821 F.2d 248 (5th Cir. 1987).

> With the advances in video technology, however, use of this most intrusive form of surveillance may increase tremendously. Thus, a detailed description of both the facts and legal analysis in the three existing cases is necessary to demonstrate how the courts have slowly relaxed the standards with which law enforcement officers must conform when using video cameras as an investigative technique. If future courts further lower these standards, law enforcement officers may be able to intrude into the most personal aspects of citizens' lives.

Troy, *supra* note 176, at 449 n.43. "Considering the world-wide fear of terrorism and the number of lives the defendants' activities endangered, the government could not have found a more compelling case for introducing video surveillance into the federal courts." *Id.* at 452.

[186] 751 F.2d at 882. The court did state that "television surveillance is exceedingly intrusive . . . and inherently indiscriminate, and . . . could be grossly abused—to eliminate personal privacy as understood in modern Western nations." *Id.*

[187] *See id.* at 877. The defendants were members of Fuerzas Armadas de Liberacion Nacional Puertorriquena ("FALN"), a group that wanted the United States territory of Puerto Rico to separate from the United States. *See id.* at 876. The FALN was responsible for a number of bombings in New

surveillance was proper, as private activities were not involved, but purely activities of an illegal nature.[188] The court stated, however, that video surveillance represents an extremely intrusive form of technology and that the constitutional standard for issuing a warrant should be placed very high.[189] The court additionally identified provisions of Title III of the Omnibus Crime Control and Safe Streets Act of 1968[190] ("Title III") that it believed were applicable to video surveillance.[191]

In *United States v. Biasucci*, the Second Circuit found support for upholding video surveillance warrants in Title III's silence in regards to video surveillance.[192] The defendants were charged by the government with violating the Racketeer Influenced and Corrupt Organizations Act ("RICO").[193] In their investigation the government sought and was granted an order authorizing video surveillance inside the defendants' place of business.[194] "Finding the reasoning of *Torres* to be compelling," the court held that "district courts, federal magistrates, and state judges may authorize television surveillance of private premises in appropriate circumstances."[195] However, the court failed to explain why video surveillance was explicitly necessary under the circumstances.[196]

York, Chicago, and Washington D.C. *See id.* Using video surveillance, the government watched as some of the defendants assembled bombs. *See id.* at 877.

[188] *See id.* at 883.

> [T]he invasion of privacy caused by secretly televising the interior of business premises is less than that caused by secretly televising the interior of a home, while the social benefit of the invasion is greater when the organization under investigation runs a bomb factory than it would be if it ran a chop shop or a numbers parlor.

Id.

[189] *See id.* at 883-84. The court noted that even video surveillance conducted pursuant to a warrant could be held to be unconstitutional if the intrusiveness of the search exceeded the necessity of using video surveillance. *See id.* at 883.

[190] 18 U.S.C. §§ 2510-2520 (1994). The Act governs audio surveillance, but does not address video surveillance.

[191] *See Torres*, 751 F.2d at 882. In the court's opinion, the Title III provisions applicable to video surveillance were the particularity of the search (18 U.S.C. § 2518(1)(b) (1994)), the necessity of using video surveillance (18 U.S.C. § 2518(1)(c) (1994)), and the time period in which the surveillance is to occur (18 U.S.C. § 2518(1)(d) (1994)). *See Torres*, 751 F.2d at 885. *See also* Troy, *supra* note 176, at 451.

[192] 786 F.2d 504, 508-09 (2d Cir. 1986). The court did not choose to analyze the surveillance under the Fourth Amendment, instead applying specific provisions of Title III that it deemed "codifications of the amendment's requirements." Cheryl Spinner, *Let's Go to the Videotape: The Second Circuit Sanctions Covert Video Surveillance of Domestic Criminals*, 53 BROOK L. REV. 469, 474 (1987).

[193] Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. §§ 1961-1968 (1982). *See Biasucci*, 786 F.2d at 506. The defendants were appealing the trial court's decision to admit video tapes recorded by surreptitious video surveillance that had been installed pursuant to a warrant issued by a district court. *See id. See also* Troy, *supra* note 176, at 452.

[194] See *Biasucci*, 786 F.2d at 507.

[195] *Id.* at 509.

[196] *See* Troy, *supra* note 176, at 453.

> Unlike *Torres*, however, *Biasucci*, does not explain why the government needed to use video surveillance in addition to other forms of electronic surveillance. In *Torres*, the government believed that audio surveillance alone would be ineffectual because the terrorists worked in

A more recent federal appellate decision involving video surveillance is *United States v. Cuevas-Sanchez*.[197] In *Cuevas-Sanchez*, the government obtained a warrant allowing video surveillance of the exterior of the defendant's home, an alleged drug dealer.[198] The government placed the video camera on a utility pole that overlooked a tall fence in the back of the defendant's property.[199] However, the Fifth Circuit rejected the government's argument that the defendant's backyard could clearly be seen from a variety of different angles, and that therefore the defendants could not have had a reasonable expectation of privacy in their backyard.[200] The court invoked principles from Title III, believing, as the *Torres* and *Biasucci* courts had, that doing so would sufficiently safeguard the defendant's Fourth Amendment rights.[201] The majority felt that the warrant had met the statutory requirements, and therefore concluded that the Fourth Amendment had been satisfied.[202]

In *Cuevas-Sanchez*, the Fifth Circuit adopted the standard from *Torres* but applied it less strictly—the video surveillance was not absolutely necessary but the court approved it anyway.[203] Neither *Cuevas-Sanchez* nor *Biasucci* appears to have balanced the necessity of the video surveillance with its level of intrusiveness.[204]

2. *Plain View Doctrine*

The plain view doctrine is an exception to the warrant requirement. If something is in plain view, there is no need for a warrant since law enforcement officials did not have to search to find it.[205] If something illegal

---

silence. In *Biasucci*, audio surveillance might have been completely adequate. The surveillance was of an office, not a home, and therefore, was probably not unreasonable balanced against the need to search.

Id.

[197] 821 F.2d 248 (5th Cir. 1987).

[198] *See id.* at 249-50.

[199] *See id.* at 250.

[200] *See id.* at 250-51.

[201] *See id.* at 251-52.

[202] *See id.* at 252.

[203] *See* Troy, *supra* note 176, at 456.

The area under surveillance was neither a safe house nor place of business but the backyard of Cuevas-Sanchez' home. The crime under surveillance was serious, but nothing in the record showed that lives had been in jeopardy. The government even argued that the warrant was unnecessary because the activity under surveillance could have been seen without a camera. The court recognized that this argument negated the necessity provision of the warrant application, but still upheld the warrant.

Id.

[204] *See id.* The courts does not appear to be balancing the type of crime involved with the place to be searched, and so would appear to be relaxing the standards for video surveillance warrants.

[205] See Coolidge v. New Hampshire, 403 U.S. 443, 465 (1971). *See also* Jennifer M. Granholm, *Video Surveillance on Public Streets: The Constitutionality of Invisible Citizen Searches*, 64 U. DET. L. REV. 687, 692 (1987).

is in plain view, an officer has the right to seize it on the spot. The doctrine only applies when something (an object or an act) is inadvertently discovered.[206] It is not applicable if the object or act has been discovered as a result of a deliberate search.[207]

3. *Open Field Doctrine*

Another exception to the warrant requirement is the open field doctrine.[208] This doctrine holds that if an item found cannot be classified as a person, house, paper, or effect, the item is not entitled to Fourth Amendment protection against search or seizure.[209] This is especially true if the owner has not taken reasonably adequate precautions to ensure privacy.[210] The doctrine often comes up in cases that involve warrantless aerial surveillance by law enforcement agencies.[211]

4. *Does the Use of Facial Recognition Technology and Video Surveillance Constitute a "Search" Under Current Law?*

Facial recognition technology is not likely to be used presently by video surveillance implemented pursuant to a "search" warrant. Normally, when law enforcement officers obtain such a warrant, they are aware of the identity of those likely to be under surveillance. There are other times when the use of facial recognition technology would be of possible benefit when used pursuant to a "search" warrant, such as when all of the suspects have not been identified. The question of whether facial recognition technology constitutes a Fourth Amendment "search" is more likely to come up when it is part of a law enforcement video surveillance system used to monitor public areas such as airport terminals, border entry points, and housing projects.

Under the *Katz* test the main factor a court will consider is the reasonable expectation of the individual to be free of surveillance in public and private.[212] While in public, most people generally expect to be observed by others to a certain extent. Individuals are aware that they are often being monitored or videotaped while in public, whether they are going to a

---

[206] *See* Harris v. United States, 390 U.S. 234, 235-36 (1968). *See also* Granholm, *supra* note 205, at 692.

[207] *See* Granholm, *supra* note 205, at 693.

[208] *See id.* at 693.

[209] *See id.* The Fourth Amendment specifically discusses "[t]he right of the people to be secure in their persons, houses, papers, and effects . . . . " U.S. CONST. amend. IV. "However reasonable a landowner's expectations of privacy may be, those expectations cannot convert a field into a 'house' or an 'effect.'" Oliver v. United States, 466 U.S. 170, 184 (1984) (White, J., concurring). *See also* Granholm, *supra* note 205, at 693.

[210] *See* Granholm, *supra* note 205, at 693.

[211] *See id.*

[212] Katz v. United States, 389 U.S. 347, 351-52 (1967).

convenience store or are in the office building in which they work. In private, particularly in the home, there is normally a much more reasonable expectation of privacy.

On the other hand, individuals are generally unaware of the sophistication of new surveillance technology and of the higher levels of intrusions into privacy that these technologies make possible.[213] Most people do not expect to be randomly observed in a crowd and have their identity and a wealth of other personal information available to observers.[214] They therefore may indeed have a reasonable expectation of anonymity and personal privacy, even while in public. Accordingly, facial recognition technology could infringe upon this expectation.

Under the plain view doctrine,[215] the issue would be whether information discovered through the use of video surveillance and facial recognition technology is inadvertently discovered, falling within the plain view of law enforcement officials. There are two factors that courts consider: first, the serendipity of the discovery; and second, whether the discovery occurs while a valid search is being undertaken.[216] Video cameras are usually used for a certain purpose—to catch illegal and illicit activity. If the cameras do so, then the discovery of the activity or item is advertent. This is especially true when the video camera is equipped with facial recognition technology and other enhancement devices such as night-scopes.

On the other hand, law enforcement agencies often use video surveillance to replace a beat cop. In this situation, video surveillance is purposely used to prevent or catch crime, which is the function of a beat cop. Nevertheless, when video surveillance does catch an illegal act, it is as inadvertent as if a beat cop were to come across something illegal occurring on his beat or, in the case of cameras used in combination with facial recognition technology, come across a wanted criminal that he recognizes.

Under the open field doctrine,[217] the location of the surveillance would not be determinative. The use of facial recognition technology to extract a facial signature from a video image can be compared to the extraction of biological samples from a person's body. Although using facial recognition technology is far less intrusive, considering that certain physiological

---

[213] *See* Dow Chem. Co. v. United States, 476 U.S. 227, 238 (1986) (noting that the sophisticated use of surveillance equipment generally unavailable to the public might be constitutionally proscribed absent a search warrant).

[214] *See* Burrows, *supra* note 33, at 1080. "Americans begrudgingly accept these surveillance devices, but few citizens expect the same surveillance on the public streets or in every private activity outside the home." *Id.*

[215] *See supra* Part V.B.2.

[216] *See* Granholm, *supra* note 205, at 697.

[217] *See supra* Part V.B.3.

information can be gleaned from an individual's facial features and patterns, the Court generally considers the gathering of individuals' physiological or biometric information by the government as a "search" under the Fourth Amendment.[218]

Under the *Torres*[219] test, courts would also consider the level of intrusiveness of facial recognition technology and video surveillance. The issue is whether it is unconstitutional to monitor people absent individualized suspicion. There is a definite dragnet quality to the use of video surveillance in this manner.[220] It is the equivalent of a mass search. The type of premises in which the video camera system is placed also would determine the level of intrusiveness. Should the premises be an individual's home where private activities occur, a court might decide that video surveillance is too invasive. In *Torres*, the sole activity monitored was illicit.[221] If the activity is partially private, a court would find a greater level of intrusion.

Courts also look to the nature of the governmental interest under the *Torres* test.[222] While it is unknown whether the Supreme Court would consider the use of facial recognition technology to gather biometric signatures as an unreasonable invasion of privacy, the Court has allowed the government to violate a person's reasonable expectation of privacy when it advances a legitimate government interest.[223] The question may then be when the need for the information supplied by facial recognition technology can be called a sufficiently legitimate and weighty interest.[224] The nature of the crime would be considered in weighing the extent of the government's interest. Use of video surveillance and facial recognition technology in public places would require weighing the government's interest against the randomness of the search and the intrusiveness of the technology.

---

[218] *See* Petti, *supra* note 74, at 723.

[219] United States v. Torres, 751 F.2d 875 (7th Cir. 1984).

[220] *See* Christopher Slobogin, *Technologically-Assisted Physical Surveillance: The American Bar Association's Tentative Draft Standards*, 10 HARV. J.L. & TECH. 383, 396-97 (1997).

> [W]hile lower courts accept the idea that a dog sniff of luggage is generally not a search, several have expressed concern over the routine use of dogs to sniff all packages in a particular area. Similarly, while aerial surveillance is generally not considered a search, courts have condemned random aerial patrols over wide-ranging areas. Along the same lines, in his dissent in *Jacobsen*, Justice Brennan cautioned against reading the Court's contraband search cases to . . . allow drug scanning devices to 'scan . . . all passersby,' or to authorize the use of such devices 'to identify all homes in which [contraband] is present.

Id. (second alteration in original) (quoting *United States v. Jacobsen*, 466 U.S. 109, 138 (1994) (Brennan, J., dissenting)).

[221] *See* 751 F.2d at 883.

[222] *See id.* at 882-83.

[223] *See* Petti, *supra* note 74, at 723.

[224] *See id.*

5. *Statutory Enactments*

On the Federal level, Congress has not yet enacted legislation to protect individuals from the widespread use of video surveillance, facial recognition, or other new surveillance technologies.[225] Courts therefore must use Title III[226] provisions to try to prevent abuses.[227]

Title III restricts aural surveillance (wire and phone taps) where there has been no consent from a party to the conversation.[228] It does not, however, specifically address or encompass video surveillance.[229] Under Title III, the requirements that law enforcement must meet to use audio surveillance (and video surveillance by analogy) are as follows: (1) probable cause, (2) particularity (type of crime, location, type of communication, and identity of surveillance subject), (3) necessity (must be able to show that other more traditional, and less intrusive forms of surveillance cannot succeed), and (4) minimization (must minimize the interception of non-relevant conversation and activity).[230] In 1986, Congress amended Title III to correspond with the good faith exception to the exclusionary rule.[231]

The Privacy Act of 1974[232] restricts the collection, use, and dissemination of personal information by federal agencies and allows individuals the right to access and correct such information.[233] The Act also controls the matching of information from several government databases ("data creep").[234] Federal employees are prohibited from disclosing any data that could incorporate an individual's biometric signature to any party that is not entitled to receive that information.[235] However, they are not prohibited from releasing the information to other federal agencies or to federal or state law enforcement agencies.[236]

---

[225] *See* Spinner, *supra* note 192, at 471-72. *See also* Burrows, *supra* note 33, at 1083. "Congress has never directly addressed the use of video surveillance on public streets." *Id.*

[226] 18 U.S.C. §§ 2510-20 (1994).

[227] *See generally* Troy, *supra* note 176, at 448-49 (discussing traditional Fourth Amendment requirements).

[228] *See* Troy, *supra* note 176, at 445.

[229] *See id.* at 448.

[230] 18 U.S.C. § 2518(1)(b) (Supp. 1986). *See also* Troy, *supra* note 176, at 448.

[231] 18 U.S.C. § 2518(10)(c) (Supp. 1986). The good faith exception was announced in *United States v. Leon*, 468 U.S. 897 (1984). If a law enforcement officer has a good faith belief that a warrant is valid, then evidence found pursuant to the warrant is not excludable. *See id.* at 919-20.

[232] 5 U.S.C. § 552a (1994).

[233] *See* REGAN, *supra* note 143, at 6. This statute prohibits disclosure of personal information "without the written consent of an individual to whom the record pertains unless the disclosure is for the purpose for which the data was collected." Petti, *supra* note 74, at 732.

[234] 5 U.S.C. § 552(a) (Supp. 1995).

[235] *See* 5 U.S.C. § 552a(b)(7) (1994); Petti, *supra* note 74, at 732.

[236] *See* 5 U.S.C. § 552a(b)(7) (1994). The head of the agency or law enforcement agency must formally request the portion of the record desired and describe the purpose for which it is desired. *See id.*

6. *State Privacy Protections*

States have the power to create rights for their citizens, beyond those granted in the Federal Constitution.[237] Proposals to regulate or terminate law enforcement's ability to use video surveillance may find their basis in state privacy rights as expressed in state constitutions or statutes.[238] Some state constitutions explicitly articulate an individual right to privacy. These states include Oregon, Pennsylvania, Alaska, Hawaii, and Montana (which employs a strict scrutiny test in cases involving privacy rights).[239] In any case, many civil liberties and criminal defense lawyers are counting on state courts, which often are more protective of individual rights than federal courts, to check the use of intrusive new surveillance technologies.[240]

The California Constitution specifically lists privacy as being an inalienable right.[241] In many of its rulings, the California Supreme Court has indicated that the scope of the protection granted by the state constitution's explicitly enumerated privacy right is sometimes greater than the scope of the United States Constitution's unenumerated right of privacy.[242] However, in the context of privacy claims by defendants in criminal trials, the California Supreme Court held that the right to privacy guaranteed by Article 1, section 1 of the California Constitution is merely coextensive with the federal right guaranteed by the Fourth Amendment.[243] In the search and seizure context, the privacy protections of the California Constitution currently apply only where parties to the conversation have a reasonable expectation of privacy with respect to what is said.[244] Thus, although the California Constitution's explicit articulation of an individual right to privacy could allow courts to check law enforcement's use of powerful new surveillance technologies, it has not yet been used in this manner.[245]

---

[237] *See* Burrows, *supra* note 33, at 1113.

[238] *See id.* State courts must have adequate and independent grounds for decisions rested on state constitutional rights and must make a plain statement that, in its judgement, the case was decided based on state constitutional law. *See id.* at 1112.

[239] *See id.* at 1113-14.

[240] *See* Hansen, *supra* note 7, at 48.

[241] CAL. CONST. art. I, § 1. "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." *Id.*

[242] *See, e.g.*, Santa Barbara v. Adamson, 610 P.2d 436, 440 n.3 (noting that the federal right to privacy "appears to be narrower than what the voters approved in 1972 when they added 'privacy' to the California Constitution").

[243] *See* People v. Crowson, 660 P.2d 389 (Cal. 1983).

[244] *See* People v. Estrada, 155 Cal.Rptr. 731 (1979).

[245] *See generally* J. Clark Kelso, *California's Constitutional Right to Privacy*, 19 PEPP. L. REV. 327 (1992) (noting that the California Constitution explicitly declares that state constitutional rights are independent of corresponding federal constitutional rights).

7. *American Bar Association Proposed Standards*

The American Bar Association ("ABA") has also proposed standards regarding "technologically assisted physical surveillance."[246] In these standards, the ABA equates video surveillance of private locations with the interception of private communications (wiretapping).[247] Under these standards, video surveillance used with facial recognition technology would be permitted if it was reasonably likely to achieve a legitimate law enforcement objective, approved by a politically accountable political official, and presented to the public with an opportunity for comment.[248] Where video surveillance is used for deterrence purposes, the ABA believes that the public must be notified of the proposed video camera and be allowed to express its views.[249] While having no legal effect, the ABA's standards constitute persuasive authority and encourage public debate over the use of video surveillance.

VI. DEBATE SURROUNDING FACIAL RECOGNITION TECHNOLOGY AND VIDEO SURVEILLANCE

A. ARGUMENTS IN FAVOR

1. *Increased Security, Declining Crime Rates*

People often accept intrusions into their privacy because they recognize the need for security in an increasingly dangerous world, and because it seems a small inconvenience and price to pay for personal safety.[250] New technologies make it easier and more economical for law enforcement to monitor public areas.[251] Facial recognition and video surveillance technology can be successful in catching criminals and preventing criminal activity. In Boston, Massachusetts, a thirty percent drop in crime in housing projects coincided with the installation of a video surveillance system.[252] By

---

[246] Slobogin, *supra* note 220, at 388. The product of the ABA's Task Force on Technology and Law Enforcement, these standards were adopted by the American Bar Association's House of Delegates in August, 1998. *See* Ward, *supra* note 33, at S8.

[247] Slobogin, *supra* note 220, at 440.

[248] *See* Hansen, *supra* note 7, at 48.

[249] *See* Ward, *supra* note 33, at S8.

[250] *See* Hansen, *supra* note 7, at 45.

[251] *See* Ward, *supra* note 33, at S4. "CCTV cameras, thus, become what the military refers to as a 'force multiplier,' inexpensive tools that allow for a greater coverage than a police department alone can provide." *Id.* at S4-S5.

[252] *See* Burrows, *supra* note 34, at 1123. In Baltimore, Maryland, data from 1996 and 1997 shows a drop in crime after the installation of video surveillance. *See* Beth Wade, *Dealing with Perception: Baltimore's Cameras Make Citizens Feel Safer*, AM. CITY & COUNTRY, Oct. 1998, at S22, S22. Likewise, in a New York City housing project, CCTV cameras are credited with a 44% drop in crime. *See* Ward, *supra* note 33, at S6.

protecting privacy and eliminating video surveillance, law enforcement is impeded to some extent.[253] The evidentiary use of video surveillance tapes in criminal trials leads to speedier trials and increased plea bargains, unclogging the court system.[254] Video surveillance and facial recognition are also capable of disproving false accusations.[255]

Video surveillance can also protect individuals from abusive actions by the police,[256] especially where surveillance is being utilized in a law enforcement capacity (and officers are therefore aware of its existence). However, where video surveillance is officially utilized, police officers are often more concerned about the cameras monitoring them, rather than the public.[257]

2. *High Public Support*

Public approval of video surveillance has risen sharply in the past few decades.[258] In 1978, only ten percent of the population felt comfortable with the concept of video surveillance programs; by 1997, that number had increased to fifty-two percent.[259] Some of the increase can probably be attributed to the creeping familiarity that constant exposure to visual surveillance breeds. The increase may also be attributable to the perception that video surveillance is an effective deterrent to crime and a necessary implement of social order. As facial recognition technology can also serve as a powerful law enforcement tool and criminal deterrent, the public might become just as comfortable with its increased use.

In those places that have already installed video surveillance systems, public support is also high.[260] In Scotland, for example, a recent survey registered support among almost ninety percent of the respondents.[261]

---

[253] This is so if only for the fact that video surveillance frees up police to patrol other areas. *See* Burrows, *supra* note 33, at 1124. "[F]ederal and state governments possess a competing interest in successfully exercising their powers of law enforcement. They argue that protections for biometric information should not compromise their ability to obtain information necessary for the prosecution of a crime." Petti, *supra* note 74, at 728.

[254] *See* Burrows, *supra* note 33, at 1124.

[255] *See id.*

[256] *See id.* at 1079-80. For example, one of the more famous examples of video camera surveillance usage was George Holiday's videotaping of the brutal beating of Rodney King at the hands of Los Angeles Police Department officers. *See id.*

[257] *See* Granholm, *supra* note 205, at 688-89. This might simply be because police officers do not wish video cameras to record them engaged in dining or leisure activities while on duty. *See also* Burrows, *supra* note 33, at 1127. "[P]olice officers become less efficient because they also do not want be watched. Law enforcement personnel frequently spend more time watching the cameras than watching the streets." *Id.*

[258] *See* Ward, *supra* note 33, at S8.

[259] *See id.*

[260] *See* Burrows, *supra* note 33, at 1124.

[261] *See id.*

To the extent that these high approval ratings rest on the perception that the world we live in is now more dangerous than it was before, public support may be misguided. Crime rates have been dropping across the United States for most crimes for a number of years.[262] However, public opinion is more strongly affected by what it perceives as "security mobilization," than by actual crime rates.[263] In other words, when people see video cameras sprouting up everywhere, they assume that the change must be warranted by circumstances.[264]

On the other hand, some Americans are worried about the loss of personal privacy, autonomy, and anonymity they seem to be experiencing.[265] The use of facial recognition technology with video surveillance may additionally raise fears of privacy loss among the general public.[266] Other public fears might include feelings that the technology will enhance the power of government or certain organizations over individuals, or that the technology will represent a "hostile symbol of authority."[267] While the public perception of crime and the need for additional law enforcement measures currently remain high, at some point additional intrusions into privacy may change popular opinion regarding video surveillance.

3. *Efficiency*

Just as facial recognition technology and video surveillance speed up the judicial process and increase law enforcement efficiency, this technology may also increase efficiency within government and private industry. For example, this technology can be used to eliminate entitlement fraud, which allows taxpayer dollars to be used more efficiently.[268] The Los Angeles County Department of Public Social Services reported that a pilot program in which finger imaging was used to identify welfare recipients

---

[262] *See* Boal, *supra* note 9, at 38.

[263] *See* DAVIS, *supra* note 8, at 224 (stating that "security" is a positional good, and has less to do with personal safety than with personal insulation from unsavory groups and individuals, or crowds in general). "Where there is an actual rising arc of street violence, as in Southcentral Los Angeles or Downtown Washington D.C., most of the carnage is self-contained within ethnic or class boundaries . . . . Surveys show that Milwaukee suburbanites are just as worried about violent crime as inner-city Washingtonians . . . ." *Id.*

[264] Certainly sensationalism brought about by competition among the media reinforces this assumption.

[265] *See* Boal, *supra* note 9, at 38 (92% of respondents told a Westin-Harris poll that they were concerned about threats to their personal privacy. This represents the highest reported level since the late 1970s.).

[266] *See* Petti, *supra* note 74, at 737. "The need to identify oneself may be intrinsically distasteful to some people . . . . [T]hey may regard it as demeaning . . . or an insult to human dignity to use a number or code instead of a name." *Id.* (quoting Roger Clarke, *Human Identification in Information Systems: Management Challenges and Public Policy Issues*, INFO. TECH. & PEOPLE, Dec. 1994, at 6-37).

[267] Petti, *supra* note 74, at 737.

[268] *See* Woodward, *supra* note 73, at 136.

saved fourteen million dollars in welfare fraud loss over a three year period.[269]

4. *Ways to Prevent Crime While Still Protecting Privacy*

Defenders of surveillance technologies often argue that it is simply a matter of balancing the public desire for a secure and safe environment with the need for personal privacy and the balance can be achieved through appropriate technological safeguards.[270] Video surveillance devices normally tape over previous recordings (or in the case of digital image recordings, delete after a certain period) if there are no reasons to keep the recordings (i.e., if no crime occurs).[271] With facial recognition technology, an individual's facial signature is supposedly deleted once it is determined that it does not match any signatures within the database.[272] The trouble that civil libertarians have with this is there is no oversight to ensure that images and identities are deleted and not instead stockpiled, then exchanged, sold, or used in the future.[273]

B. ARGUMENTS AGAINST

1. *Privacy Invasion*

There is no question that the use of video surveillance and facial recognition technology eliminates some amount of personal privacy and anonymity. Surreptitious video surveillance can be used to monitor behavior without the knowledge of the subject. Facial recognition technology can use the images taken from video surveillance to obtain a subject's identity and personal information.

---

[269] *See id.* at 98.

[270] *Cf.* Burrows, *supra* note 33, at 1124.

> If it turns out that camera operators are peering into shops and apartments, the cameras can be programmed to simply not register those areas. Alternatively, a computer alarm could notify a supervisor of the operator's activities. To discourage unauthorized distribution of information, Baltimore, Maryland, destroys or recycles tapes after 96 hours and Tacoma, Washington, does not even use tapes.

Id.

[271] *See id.* "If it turns out that camera operators are peering into shops and apartments, the cameras can be programmed to simply not register those areas. Alternatively, a computer alarm could notify a supervisor of the operator's activities. To discourage unauthorized distribution of information, Baltimore, Maryland, destroys or recycles after 96 hours and Tacoma, Washington, does not even use tapes." *Id.*

[272] *See Find Criminals*, *supra* note 60.

[273] *Cf.* Boal, *supra* note 9 (noting that "[w]hat alarms civil libertarians is that 'no one knows what happens to the tapes once they are recorded, or what people are doing with them'").

2. *Chilling Effects on Human Behavior: The New "Panopticon"*

People become resigned to video surveillance and the prospect of being watched—they become complacent and apathetic to the loss of autonomy.[274] People unconsciously take less risk when they think they are the subject of video surveillance because they do not wish to offend the bland sensibilities of whoever might be watching them on the other end. If individuals become aware that their personal identity and information can be accessed along with an image of their face, they will be even further inhibited in their actions and words.

A central concept behind social control theory is the authority of the watcher over the watched.[275] When people are subjected to scrutiny, they are likely to act in ways that make them indistinguishable from the next person.[276] Lovers walking through a park are not likely to hold hands if they know they are being watched, let alone bring a blanket and a bottle of wine. "[M]ass monitoring works like peer pressure, breeding conformity without seeming to."[277]

Jeremy Bentham, an eighteenth century philosopher, believed that the anxiety of constant surveillance was such a powerful molder of human behavior that he made it the basis for his plan for a humane prison system.[278] In his proposed prison, prisoners' behavior would be controlled through the knowledge that their every action was being observed.[279] Bentham called this instrument of conformity the *Panopticon*.[280]

The philosopher Michel Foucault likewise believed that the threat of constant surveillance was a crucial organizing feature of modern, complex societies.[281] According to Foucault, the conformity instilled on individuals through the prospect of constant observation is how societies achieve social cohesion and coherence.[282] As a consequence, individuals under constant video surveillance wind up paying a heavy psychological price for social stability.[283]

---

[274] *See* Meeks, *supra* note 11, at 11.

[275] *See* Boal, *supra* note 9, at 38.

[276] *See id.* A possible exception to this might be the born extroverts, those among us who must act when presented before a camera.

[277] *Id.*

[278] *See* JEREMY BENTHAM, THE PANOPTICON WRITINGS 33 (Miran Bozovic ed. 1995).

[279] *Id. See also* Boal, *supra* note 9, at 38.

[280] *See* Boal, *supra* note 9, at 38.

[281] MICHEL FOUCAULT, DISCIPLINE AND PUNISH 213-14 (Alan Sheridan trans., Vintage Books 2d ed. 1995) (1975). *See also* Boal, *supra* note 9, at 38.

[282] *See* FOUCAULT, *supra* note 281, at 213.

[283] *See id.* at 214.

3. *Growth of the "Police State"*

Facial recognition technology and video surveillance greatly enhance the capabilities of modern law enforcement agencies. With the end of the Cold War, the military has become involved in law enforcement in certain limited capacities.[284] Additionally, many surveillance technologies developed by the military have been put to use in law enforcement capacities.[285] There is also the chance that the military and national security forces will continue to become more involved in domestic policing, as they seek to ensure their organizational existence.[286]

4. *Discriminatory Targeting of Certain Groups*

"'Once the new surveillance systems become institutionalized and taken for granted in a democratic society,' they can be 'used against those with the 'wrong' political beliefs; against racial, ethnic, or religious minorities; and against those with lifestyles that offend the majority.'"[287] For example, in Miami Beach, the use of public video surveillance for law enforcement purposes was started only after lower-income black and Hispanic citizens began residing in the community of elderly retirees.[288]

Social psychologists have also determined that videotaping participants in political activities affects their sense of self, because there is a tendency to unconsciously associate being surveilled with criminality.[289] Individuals may be less willing to become involved in political activities if they know that they will be subject to video surveillance, and possibly arrest. In this manner, the use of video surveillance can be used to obstruct the political speech and associational rights of individuals and groups that engage in political activities.

5. *Loss of Property Interest in Personal Identity and Photographic Image*

Gary Marx, a professor at the Massachusetts Institute of Technology specializing in privacy issues, has proposed that Congress establish a royalty system to compensate individuals, or consumers as a group, whenever personal information about them is sold.[290] "[I]t seems only fair

---

[284] *See* Andreas, *supra* note 13, at 41-42.

[285] *See id.*

[286] *See id.* at 42.

[287] *See* Boal, *supra* note 9, at 38 (quoting author Gary T. Marx, professor at the Massachusetts Institute of Technology).

[288] *See* Burrows, *supra* note 33, at 1082. The surveillance was begun in 1982 and discontinued in 1984, after failing to catch a single criminal. *See id.* at 1080-82.

[289] *See* Boal, *supra* note 9, at 38 (surmising that ordinary citizens will stay away from engaging in political activities when they commonly see activists subjected to the scrutiny of video surveillance—no one wants to be on the nightly news or in a police video).

[290] *See* Richard Lacayo, *Nowhere to Hide: Using Computers, High-Tech Gadgets and Mountains of Data, an Army of Snoops Is Assaulting Our Privacy*, TIME, Nov. 11, 1991, at 34, 40.

that those to whom it pertains ought to control it and share in financial gain from its sale."[291] This would conceivably apply to photographic and video images as well, although only where the images are sold. There are also ethical dilemmas associated with capturing someone's facial image and storing it in a database without either their permission or informed consent.

6. *Security of Information, Databases*

The term "data creep" describes the way in which information given and used for one purpose, such as public records, tends to be disseminated—from the governmental agency that collects the information to a company that compiles databases of information, and then finally to the consumers of this information.[292] There are fears that information collected through video surveillance and facial recognition technology (combined with other potential sources of data) will be shared among governmental agencies and outside entities.[293]

There are also concerns about the inappropriate use of video surveillance and facial recognition software by those who are doing the monitoring. There have been numerous incidents of police observers being disciplined for directing the gaze of video cameras towards inappropriate areas of civilians' anatomy or through bedroom windows.[294]

7. *Reliability of Technology*

Individuals have previously been arrested and prosecuted based on video surveillance footage, then later released after police realized that they had mistakenly arrested the wrong person.[295] Digitization also allows for the imposition or removal of an individual's image into video surveillance footage.[296] Even experts in the technology are unable to recognize a digital reproduction from its original.[297] Therefore there is a significant danger that

---

[291] *Id.* (quoting Gary T. Marx, professor at the Massachusetts Institute of Technology).

[292] *See* Tom Kisken, *Smile, You're on Someone's Camera. Watchdogs Warn: Society Becoming Video Fishbowl*, ST. J-REG., July 1, 1998, at 27; *see also* Petti, *supra* note 74, at 726-27.

[293] *Cf.* Kisken, *supra* note 292, at 27 (noting that "names and addresses obtained for one purpose such as a product warranty or public records only to be sold to database companies who pass on the information to sales people, private detectives, lawyers investigating lawsuits or anyone else"); Petti, *supra* note 74, at 727-28. "Identifications systems implemented in the United States have a history of "function creep," the application of the identification scheme to additional purposes not announced or intended at the beginning of the plan." *Id.* at 726.

[294] *See* Boal, *supra* note 9, at 38 (describing how a female police sergeant in Brooklyn, New York turned in fellow officers for using a camera to take pictures of women's breasts and backsides).

[295] *See* Burrows, *supra* note 33, at 1127. Of course, mistaken arrests also occur with eyewitness identifications. The incidence of mistaken arrest resulting from video surveillance footage is likely lower than with eyewitness identification. Of course, police and juries are more likely to trust identifications based upon video surveillance footage.

[296] *See id.*

[297] *See id.*

video surveillance footage can be "doctored" to include or remove incriminating images.

8. *Does Not Prevent, but Displaces Crime*

Researchers disagree about the value of video surveillance and facial recognition technology in deterring crime.[298] Statistics show that very few cities undergo a drop in crime where video surveillance systems are in operation.[299] Some argue that, if anything, law enforcement use of surveillance technologies merely displaces criminal activities outside of the range of the camera.[300] Officers in areas where video surveillance is used have also expressed this opinion, stating that the criminal element simply moved their activities outside of the camera's range.[301]

While some crime may be displaced, there is a possibility that impulsive crimes (vandalism, graffiti, etc.) may be reduced if the presence of the video surveillance system is well known.[302]

9. *Interference with Rights of Free Speech and Association*

One of the most fundamental objections to the constant presence of video surveillance is that it destroys the character and spontaneity of a free and vibrant citizenry.[303] When people know they are being watched, they are not likely to conduct themselves in a way that could draw negative attention.[304] They might therefore be unwilling to act in ways that could be construed as suspicious or abnormal.[305] The atmosphere quickly becomes

---

[298] *See* Boal, *supra* note 9, at 38 (describing how more than 25 years ago, then New York City Mayor Lindsay installed video cameras in Times Square but took them down when they resulted in only ten arrests in eighteen months, and questioning Mayor Guiliani's far more ambitious current surveillance plans).

[299] *See* Burrows, *supra* note 33, at 1128. Most video surveillance systems are part of a number of other security measures, so the effect of video surveillance on crime levels is hard to isolate. New York City (Times Square), Atlantic City, and Miami Beach have labeled the surveillance cameras a failure and dismantled them. *See id.*

[300] *See 48 Hours: I Spy; Surveillance Cameras Used on City Streets to Help Cut Down on Crime Seen as Invasion of Privacy by Some*, (CBS television broadcast, Apr. 9, 1998) (interviewing John Crew, an attorney with the American Civil Liberties Union). *See also* Burrows, *supra* note 33, at 1127.

> Furthermore, studies show that surveillance cameras merely displace crime rather than deter it. Criminals simply move out of the range of the camera eye and take the crime with them. One video surveillance proponent indicated that "[o]ur experience in many cases is that the criminals tend to move their drug dealing to more private areas." Moreover, some criminals learn all of the camera locations and simply focus their activities on other less protected areas of the city.

Id.

[301] *See* Granholm, *supra* note 205, at 689.

[302] *See* Ward, *supra* note 33, at S6.

[303] *See* Granholm, *supra* note 205, at 708.

[304] *See id.*

[305] *See id.*

one of conformity and the public street stops serving as a refuge of anonymity.[306]

Video surveillance and facial recognition technology may be subject to attack on First Amendment grounds where used to monitor political activity and expression, as unnecessarily chilling freedom of speech and association.[307] However, the Supreme Court has never considered a "chilling effect" as a sole basis for prohibiting state action.[308] If the state action merely has the incidental effect of inhibiting First Amendment rights while regulating a subject within the state's power, and the impact on free speech and association is relatively small compared with the need to regulate the conduct at issue, then the state action is generally upheld.[309] All that is required is that the state demonstrates a sufficiently weighty governmental interest.[310] Of course, curbing crime would be considered by most courts to be an important state interest. There still remains the question of whether less intrusive means than video surveillance and facial recognition technology would be better able to further the government's interest.

VII. CONCLUSION

A. THESIS REEXAMINED

Currently, it seems unlikely that the Supreme Court would characterize public video surveillance by law enforcement agencies as a "search" within the meaning of the Fourth Amendment, because the Court has said that there is no reasonable expectation of privacy on public streets.[311] Whether a Constitutional "right to privacy" will affect the wide implementation of facial recognition technology and video surveillance depends on the extent and uses of the surveillance program.[312] If facial recognition technology or some other biometric identifier ever became so pervasive as to become a virtual national identification device, federal and state courts might fight a way to invalidate it, in the fear that the government would be able to track the every move of each citizen.[313] However, the social security number is now used as a de facto national identification device.[314]

---

[306] *See id.* at 709-10.

[307] *See id.* at 710.

[308] *See id.*

[309] *See, e.g.*, Younger v. Harris, 401 U.S. 37, 51 (1971).

[310] *See id.*

[311] *See* Burrows, *supra* note 33, at 1090.

[312] *See* Petti, *supra* note 74, at 726. This presumably includes the corresponding public perception and response to the program.

[313] *See id.*

[314] *See id.* The government does not yet have the ability to track every individual's movements with their social security number. "Today, private enterprises and universities along with the government use the social security number as identification." *Id.* at 727.

Some have advocated a total abolition of privacy, believing that unless the technology and access become ubiquitous, government and law enforcement will be able to use the technology for repressive purposes.[315] This ignores the psychological pain of living in a world with no privacy.[316] It might also lead to the creation of a privacy criminal, a person who dares to maintain a semblance of personal privacy.[317]

There is a common tendency to be impressed and mesmerized by the capabilities of new technology, and not to consider the changes that it brings and what is given up.[318] However, the capabilities of facial recognition technology used with video surveillance are such that it renders personal identity and many forms of human behavior completely transparent.[319] Privacy "freaks" who deride the loss of privacy in modern society are therefore right in one sense—even if you don't do something wrong, you may still have plenty to worry about.[320]

B. A GENERAL RIGHT TO PRIVACY

The Supreme Court's "fundamental rights" jurisprudence may suggest that certain areas of individuals' lives are "sacred" and outside the purview

---

[315] *See* Meeks, *supra* note 11, at 11. David Brin, an author interviewed in the February 1996 issue of WIRED, believes that "the only alternative is to give the birdlike power of sight to everybody." Sheldon Teitelbaum, *Privacy Is History—Get Over It*, WIRED, Feb. 1996. It is also possible that there will come a point when everyone has his life activities recorded on his own 24-hour web cam. But many people feel that even self-exposure, "like the kind performed by those on *Oprah* or in the modern memoir, degrades those who do it and often betrays others." Horn, *supra* note 142, at 58.

[316] *See* Meeks, *supra* note 11, at 11.

[317] *See id.*

[318] *See* Hon. Justice M.D. Kirby, *Access to Information and Privacy: The Ten Information Commandments*, 55 U. CIN. L. REV. 745, 753 (1987). "Lulled by a trivializing diet of soap operas, cowboy westerns, and Manhattan gun battles, people become indifferent spectators to or even conspirators in the erosion of their own freedoms." *Id.*

[319] *See* Woodward, *supra* note 73, at 134.

> Any high-integrity identifier [such as facial recognition technology] represents a threat to civil liberties, because it represents the basis for a ubiquitous identification scheme, and such a scheme provides enormous power over the populace. All human behavior would become transparent to the state, and the scope for non-conformism and dissent would be muted to the point envisaged by the anti-Utopian novelists [Orwell and Huxley, among others].

Id. (quoting Roger Clarke, *Human Identification in Information Systems: Management Challenges and Public Policy Issues*, INFO. TECH. & PEOPLE, Dec. 1994, at 6, 34). *See also* Boal, *supra* note 9, at 38. "Europeans know all about internal passports, but not even the East German Stazi could observe the entire population at a keystroke. 'What the secret police could only dream of,' says privacy expert David Banisar, 'is rapidly becoming a reality in the free world.'" *Id.*

[320] The possible abuses of facial recognition technology and video surveillance are endless. Privacy groups are strong advocates for privacy protections on personal information, and are opposed to the use of facial recognition technology and video surveillance (along with other biometric identification technologies) since they believe that these technologies whittle away at our privacy rights. *See* Petti, *supra* note 75, at 727-28. "Their strongest criticism concerns the possible existence of a databank composed of the biometric signatures used by ordinary people in their daily commercial and private transactions." *Id.* at 728. These privacy groups include The Electronic Freedom Foundation ("EFF"), The Center for Democracy and Technology ("CDT"), The Electronic Privacy Information Center ("EPIC"), and Computer Professionals for Social Responsibility ("CPSR"). *See id.* at 727 n.150.

and control of the government.[321] Freedom from unreasonable government video surveillance and use of facial recognition technology would be an appropriate area in which to extend this concept.[322] The future of constitutional privacy protection may, however, be limited to the areas of family and contraception, under the current Court.[323] Before the use of facial recognition and other biometric technologies become widespread, it would be wise to develop a legal and moral framework that finds an appropriate balance *between the public and private.*

Currently, there is no case or statutory law that adequately deals with new biometric technologies, or even with video surveillance. In these times of constant, swift transformation and complex science and technology, there should be greater protections for individual privacy and autonomy. A general right to privacy (or the extension of privacy rights to public areas)[324] would perhaps be able to adjust to rapidly emerging new technologies and societal changes with the necessary flexibility.

---

[321] *See id.* at 727.

[322] *See id.*

[323] *See id.*

[324] This could be accomplished by recognizing that persons do have certain expectations of privacy, even while in public, and that these expectations are inherently and objectively reasonable.