INFORMATION PRIVACY AS A FUNCTION OF FACIAL RECOGNITION TECHNOLOGY AND WEARABLE COMPUTERS

Woodrow Barfield[1]

ABSTRACT

As technological advances are made in the design of smart sensors, the issue of privacy in public places, first discussed by Warren and Brandeis in 1890, becomes an important topic for law and policy. This paper examines issues of privacy that are impacted when an individual's image is recorded by a video-based wearable computer, analyzed using facial recognition software, and uploaded to the internet. While the Constitutional basis of search and seizure law for individual's placed under video surveillance is reviewed, a particular focus of the paper is on a less investigated but emerging area of concern, the video recording and facial recognition of individuals in public places by non-government actors. The paper presents an overview of the law as applied to the use of video systems for surveillance, reviews facial recognition techniques, and discusses cases arising under state law dealing with video recording of individuals in public places. The paper concludes with recommendations for the protection of privacy calling for the legislation enactment of an information privacy statute to cover the disclosure of private information for individuals filmed by wearable computers equipped with facial recognition software.

TABLE OF CONTENTS

---

[1] Woodrow Barfield, received a Ph.D. in Industrial and Systems Engineering from Purdue University, a J.D. from the University of North Carolina, and a LL.M. in Intellectual Property Law and Policy from the University of Washington. He has served as Professor of Engineering at the University of Washington and Virginia Tech. The author thanks William Covington for helpful comments on an earlier draft of the manuscript and David Orange and Jessica Barfield for assistance in legal research. The views expressed are solely those of the author.

I. INTRODUCTION

This paper examines privacy issues that occur when video-based wearable computer systems equipped with facial recognition software are used to film an individual in a public place. Video-based wearable computers pose a significant threat to an individual's privacy- not only can wearable computers with facial recognition software record and analyze a person's face, they can be used to upload an image to the internet where it may be viewed by anyone with access to a computer and internet connection. Once the identity of a person is known, information about the person that is accessible on the internet can be presented with the individual's face.[2] The ability to film, identify, and track an individual within a public place, along with the ability to pair personal information to an individual's image, has prompted some legal scholars into calling for a new statute, covering information privacy, to provide relief for people who have had their privacy violated by computing and communications technology.[3]

The Supreme Court has broadly defined privacy as "the individual's control of information concerning his or her person," that is, the right to control the dissemination of information about oneself.[4] Similarly, information privacy involves an individual's

---

[2] *See generally Jerry* Kang, *Information Privacy in Cyberspace Transactions*, 50 Stan. L. Rev. 1193 (1998); Jerry Kang & Dana Cuff, *Pervasive Computing: Embedding the Public Sphere*, 62 Wash. & Lee L. Rev. 93 (2005). Once an individual's image is identified and uploaded to the internet, various items of personal information available on computer databases can be pieced together, resulting in a comprehensive picture of an individual.

[3] Kang, *id*. (discussing the concept of an information privacy statute).

[4] *U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 763 (1989).

personal information and his ability to control that information.[5] The basic argument for information privacy stems from the concern that individuals have a right to exert some control over who has access to their personal information, and for what purpose.[6] As expressed by a leading scholar on the topic, examples of personal information includes data assigned to an individual, such as their social security number, address, or telephone number; and information about an individual that is generated on a day-to-day basis, such as records of bank transactions, credit card purchases, phone calls, and medical treatments.[7] Other personal information may be school or medical records, employment histories, arrest records, and tracking information, as well as personal likes and dislikes. Essentially, this collection of information not only defines who a person is but in many cases describes the intimate details of a person's life; therefore to allow such information to be used without an individual's consent, especially if paired to a person's image posted on the internet, would represent an unwarranted and unprecedented invasion into a person's privacy.

As society becomes dependent on computer databases and electronic record-keeping, an individual's ability to control who has access to his personal information is becoming even more tenuous.[8] In the age of the internet and wirelessly networked wearable computers, the inability to control the dissemination and use of personal information gives rise to the issue of information privacy which may be exacerbated by video-based systems with facial recognition software. Past thoughts on information

---

[5] *See generally* Kang, *supra* note 2; Kang & Cuff, *supra* note 2.
[6] *Id*.
[7] Thomas Kearns, *Technology and the Right to Privacy, The Convergence of Surveillance and Information Privacy Concerns*, 7 Wm. & Mary Bill Rights J. 975 (1999).
[8] *See generally* Sheri A. Alpert, *Privacy and Intelligent Highways: Finding the Right Way*, 11 Santa Clara Computer & High Tech, L.J. 97, 106-107 (1995).

privacy indicated that the concept was tied to the concept of anonymity,[9] that is, the control of personal information.[10] It was not thought to address an individual's actions and movements. However, since an individual's image may be recorded as they move about a public place, their identity known and analyzed as a result of facial recognition software, and their image uploaded to the internet, this article argues for an expansion of the concept of information privacy to include the actions and movements of an individual when paired to the presentation of personal facts about the individual.

One concern resulting from the ability to identify a person and track their movements using wearable computers is that a person's right to freely travel and associate may be severely impacted and curtailed. This is because an individual who suspects that they are being filmed, and identified by strangers, may no longer feel free to move through public places speaking with whom they wish and attending the meetings that they wish.[11] For instance, according to the Supreme Court, a woman has a protected liberty interest in seeking an abortion,[12] but this right is infringed upon when someone

---

[9] Quentin Burrows, *Scowl Because You're On Candid Camera: Privacy and Video Surveillance*, 31 Val. U. L. Rev. 1079, 1125 (1997). Humans have a fundamental belief in the right to personal autonomy which stems from dignity and individuality. When the sphere of autonomy is consistently violated, the shell of humanity erodes.

[10] Kang, *supra* note 2; Kang & Cuff, *supra* note 2.

[11] The Supreme Court has expressly recognized that a right to freedom of association and belief is implicit in the First, Fifth, and Fourteenth Amendments. This implicit right is limited to the right to associate for First Amendment purposes. It does not include a right of social association. The government may prohibit people from knowingly associating in groups that engage and promote illegal activities. The right to associate also prohibits the government from requiring a group to register or disclose its members or from denying government benefits on the basis of an individuals current or past membership in a particular group. There are exceptions to this rule where the Court finds that governmental interests in disclosure/registration outweigh interference with First Amendment rights. The government may also, generally, not compel individuals to express themselves, hold certain beliefs, or belong to particular associations or groups; *see NAACP v. Alabama*, 357 U.S. 449 (1958); *Abood v. Detroit Board of Education*, 433 U.S. 915 (1977).

[12] *Roe v. Wade*, 410 U.S. 113 (1973); *Planned Parenthood of Southeastern Pa. v. Casey*, 505 U.S. 833 (1992). In Casey, the Court found it appropriate to allow information to be reported about the women receiving abortions to state agencies, as long as the actual identity of the women remained confidential. *Id.* at 900. However, by being able to film all women entering a clinic, identity is discernable and capturable along with other potentially embarrassing personal information. *Id.*

invades the woman's privacy by filming her entering a clinic from a superhuman vantage point.[13] The intrusion becomes even greater if the images are saved for some later use.[14] Once a person knows that when they enter a public place their image may be recorded and analyzed, such knowledge may chill their desire to associate, especially with causes that are counter to stated government policies; such a result would be a severe blow to a democratic society. It seems intuitive that the law should recognize the difference between being seen in public by someone with their naked eyes, versus being filmed by unknown individuals using wearable computers and having their image uploaded to the internet and identified by strangers.[15] Given the capabilities of video-based wearable computer technology to film and track individuals, the law should provide for the protection of an individual's privacy when personal information about that individual may be easily accessed on the internet and paired to the person's image posted on the internet.

As stated by several commentators, as society becomes more information-based, and as more information about an individual is available on the internet; and as the need for individuals to distribute their personal information increases;[16] the need to protect such personal information intensifies.[17] This article reviews the privacy protection people

---

[13] *See Planned Parenthood v. Aakhus*, 14 Cal.App.4th. 162 (Cal. Ct. App. 1993) (finding that photographing and videotaping clients violated the right to privacy under the California Constitution); *Chico Feminist Women's Health Ctr. v. Scully*, 208 Cal.App.3d 230 (Cal. Ct. App. 1989) (upholding an injunction against abortion protesters photographing license plates and people entering or leaving an abortion clinic).

[14] *See generally* Maureen O'Donnell, *Cameras Around Every Corner*, SUN-TIMES (Chi.), Feb. 18, 1996 at 2. It has been reported that in Alaska residents using home computers can create a news letter with still photographs of potential criminals, *see Court Allows States To Throw The Book*, *available at* http://www.cbsnews.com/stories/2003/03/05/supremecourt/main542863.shtml (last visited Jan. 27, 2006).

[15] *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, 1041 (1995).

[16] Kang, *supra* note 2; Kang & Cuff, *supra* note 2.

[17] Kang, *supra* note 2; Kearns, *supra* note 7; McClurg, *supra* note 15.

may expect to receive under current law when their image may be recorded, analyzed, and posted on the internet, and when they may be tracked in public places by individuals using wearable computer technology. The article concludes that the current law is insufficient to protect the privacy of individuals in the age of wirelessly networked wearable computers equipped with facial recognition software. As a result, the article calls for an expansion of the concept of an information privacy statute as expressed by Professor Kang,[18] and for legislative action at the state or federal level to enact a comprehensive statute which would protect the information privacy rights of individuals in public places.

EARLY THOUGHTS ON PRIVACY

In the classic article by *Warren and Brandeis* on privacy written in 1890, the proposition that privacy was a basic right was introduced.[19] After exploring the nature and scope of the right to privacy, *Warren and Brandeis* concluded that "it is the unwarranted invasion of individual privacy which is reprehended, and to be, so far as possible, prevented."[20] Now days at the bank or at the mall,[21] on the highway,[22] at a grocery store,[23] at a sports event,[24] or even walking down a street,[25] an individual's

---

[18] Kang, *supra* note 2.

[19] Samuel Warren & Louis, D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890); *but see* Richard C. Turkington, *Legacy of the Warren and Brandeis Article: The Emerging Unencumbered Constitutional Right to Informational Privacy*, 10 N. Ill. U. L. Rev. 479, 482 n.5 (1990) (indicating that a 1881 Michigan case and other sources discussed the right to privacy prior to the publication of the Warren & Brandeis article).

[20] Warren & Brandeis, *id.* at 215.

[21] Marcus Nieto, *Public Video Surveillance: Is It An Effective Crime Prevention Tool*? *Available at* http://www.library.ca.gov/CRB/97/05/ (last visited Jan, 26, 2006).

[22] *See generally* Woodrow Barfield & Thomas Dingus (eds.) *Human Factors in Intelligent Vehicle Highway Systems* (Lawrence Erlbaum Press, 1997).

[23] *State v. Dunn*, Slip Copy, Tenn.Crim.App., 2004 Tenn.Crim.App LEXIS 854 (2004) (defendant pled guilty to theft from a grocery store, the crime was recorded with a video camera which showed the defendant loading shopping carts full of groceries and leaving the store without paying); *see State v. James,* Minn.App. LEXIS 1155 (Minn.App. 2004) (evidence of the robbery of a convenience store was based on sister's identification from surveillance video).

privacy can be severely compromised as they are unknowingly filmed by a host of video cameras, some containing facial recognition software.[26]

Since the *Warren and Brandeis* article was first written, the technology which can be used to capture a person's image, track their movements, and therefore intrude upon their privacy has improved dramatically. One significant difference regarding video technology today compared to just a few years ago, is that once an individual's image is recorded, it can be subjected to analysis by facial recognition software and compared to millions of images stored in government and private databases.[27] That is, facial recognition technology[28] coupled with video cameras can be used to take pictures of individuals in a crowd which can then be compared to the facial features of known individuals, using standard biometric measurements. With video-based wearable computers, no longer will an individual be able to move within a public place with some degree of anonymity, instead once they are filmed, they can be subjected to analysis by facial recognition software and identified, thus losing any anonymity they may have had. In addition, once an individual's image is captured using video cameras, the image can be manipulated in various ways; for example, it is relatively easy to insert a digital image into film, video, or a picture in such as way as to create a false or misleading impression

---

[24] Jack Carey, USA TODAY, *ACLU Protests High-tech Super Bowl Surveillance,* 02/06/2002, *available at* http://www.usatoday.com/tech/news/2001-02-02-super-bowl-surveillance.htm (last visited Jan. 26, 2006).

[25] Steve Mann, *Sousveillance and Cyborglobs: A 30 year Empirical Voyage Through Ethical, Legal, and Policy Issues*, 14 Presence: Telerobotics and Virtual Environments 625 (2005).

[26] A person may be filmed at a border entry by a government agency, or by a non-governmental actor such as the owner of a store at a mall, or by an employer at a workplace. But the fact that a person may be "surveilled" by a non-government source may not mean that the individual's image is not accessible by the government, as the state can buy or subpoena private data, Kang & Cuff, *supra* note 2, at 127; *see also* http://www.law.ucla.edu/kang/gigs/iLaw%202004%20privacy/politics.html#Topic69 (last visited Jan. 26, 2005).

[27] In the government context, the IRS may be interested in viewing the video of a tax delinquent making a large consumer purchase.

[28] *See generally* Ric Simmons, *The Powers and Pitfalls of Technology: Technology-Enhanced Surveillance by Law Enforcement Officials*, 60 N.Y.U. Ann. Surv. Am. L. 711 (2005).

that a particular person was at a particular place at a particular time.[29] This illustrates the point that video images can be used for purposes far beyond the individual's original consent, if consent were given at all.

Based on the pervasiveness of video equipment, the relevant question to ask is not: Am I being filmed?[30] Instead, the relevant question to ask is: Who is doing the filming, and what is being done with my image? These questions are timely given the increased technological capabilities to film individuals in public places, analyze their faces using software, transmit that person's image using the internet to anywhere in the world, and track their movements. Video technology with facial recognition software, combined with the ability to search the internet for personal information about an individual, along with the ability to track an individuals movements in public places, all combine to threaten an individuals privacy in ways well beyond that discussed by *Warren and Brandeis*[31] when they called for new law to account for privacy violations resulting from recent technology advances.

II. WEARABLE COMPUTERS

The type of wearable computer that is the focus of this article consists of a small portable computer worn on the body which contains a miniature camera for video

---

[29] Seanna Browder, *Now, The Cops are Strapping on Computers*, Bus. Wk., July 13, 1998, *available at* http://www.businessweek.com/1998/28/b3586110.htm (last visited Jan. 29, 2006) (reporting field-testing in three cities of lightweight wearable computers for use in police investigation; computers are equipped with digital cameras and laser range finders for recording crime-scene data).

[30] In the context of privacy rights in the information age, it is interesting to note the sentiment expressed by Scott McNealy, CEO of Sun Microsystems, in a question posed to him about online privacy he answered: "You have zero privacy anyway. Get over it," *available at* http://www.techcentralstation.com/051500C.html (last visited Jan. 26, 2006).

[31] Warren & Brandeis, *supra* note 19.

capture, a head-worn display,[32] input device, and a wireless internet connection. The main benefit of a wearable computer is that it allows an individual to access information at any time and any place.[33] Wearable computers are especially useful for applications that require computational support while the user's hands, voice, eyes or attention are actively engaged with the physical environment. Depending on the application, the primary input to a wearable computer might be a chording keyboard, gesture, or speech recognition. There are different kinds of technology that may be considered a wearable computer, for example, a watch containing a calculator is a wearable computer as is a portable GPS unit. However, only some forms of wearable computers pose a threat to an individual's privacy- essentially those that contain a video camera or those that track a person's location.

The internet combined with advances in wearable-computer technologies, makes the comments of *Warren and Brandeis* on the unwarranted invasion of an individual's privacy even more applicable to current times.[34] With wearable computing technology,[35] a person walking down the street can unknowingly have their image captured by a miniature video camera worn by another person, and through a wireless network, have their facial image appear on the stranger's web page accessible to millions, all without

---

[32] Wearable computers are often integrated into the user's clothing or can be attached to the body through some other means, like a wristband. They may also be integrated into everyday objects that are constantly worn on the body, like a hands-free cell phone.

[33] *See generally* Steve Mann & Woodrow Barfield, *Introduction to Mediated Reality*, 15 International Journal of Human-Computer Interaction 2 (2003) (discussing the promise of wearable computers and mediated reality).

[34] Warren & Brandeis, *supra* note 19.

[35] Steve Mann, *Wearable, Tetherless Computer—Mediated Reality: WearCam as a Wearable Face-Recognizer, and Other Applications for the Disabled*, *available at* http://wearcam.org/vmp.htm (last visited Jan. 24, 2006). Edward O. Thorp, *The Invention of the First Wearable Computer*, *available at* (*http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?isnumber=15725&arnumber=729523&count=30&index=1*) (last visited Jan. 26, 2006), also in *The Second International Symposium on Wearable Computers: Digest of Papers*, IEEE Computer Society, 4-8 (1998).

their knowledge or express consent.[36] A video-based wearable computer that is wirelessly networked poses new and compelling privacy concerns for individuals in public places and raises a host of legal questions; for example, does an individual have a right to consent to their image being filmed and subjected to analysis by facial recognition software; and does a person have a right to stop an individual from posting their image on the internet?

Due to the invasiveness of facial recognition software coupled with the video capability of wearable computers, some technologists have argued for the creation of privacy faces, which could be emitted electronically by any individual with the appropriate technology.[37] The use of a privacy face would allow only certain types of data for a particular individual to be accessible by another's computing system.[38] The use of such technology represents a technological solution to the problem of having an image recorded and uploaded to the internet without consent, but such a solution is inapplicable to the vast majority of people who enter public places without the aid of technological devices to protect their privacy.

VIDEO SURVEILLANCE AND DATABASES

One threat to an individual's privacy is the fact that the use of facial recognition software, in combination with wider use of video surveillance, may grow increasingly

---

[36] *See generally* Woodrow Barfield, Steve Mann, Kevin Baird, Francine Gemperle, Chris Kasabach, John Stivoric, Malcolm Bauer & Richard Martin, *Computational Clothing and Accessories*, in Fundamentals of Wearable Computers and Augmented Reality, Woodrow Barfield & Thomas Caudell (eds.) (Elsevier Press 2001). *See also* J. Spence (dissent) in *Gill v. Hearst Publishing Co.,* 40 Cal.2d 224, 227 (1953) (arguing that placing oneself in the public view does not mean consenting to your image being observed by millions.)

[37] Kang, *supra* note 2; Kang & Cuff, *supra* note 2, at 136-137; *see, e.g*., Scott Lederer, Anind K. Dey & Jenifer Mankiff, *Everyday Practices in Ubiquitous Computing Environments, available at* http://guir.berkeley.edu/pubs/ubicomp2002/privacyworkshop/papers/lederer-ubicomp 02-workshop.pdf (discussing the use of privacy faces) (last visited Jan. 24, 2006).

[38] Kang & Cuff, *id*. at 136.

invasive over time. In theory, a positive benefit of wearable computer systems combined with video is to allow law enforcement to scan through thousands of faces in a crowd and then alert officers to the presence of any known fugitives that might be present. However, once installed, a video surveillance system rarely remains confined to its original purpose, and instead often expands in ways that threatens privacy. As new ways of using video surveillance and facial recognition systems suggest themselves, the authorities or operators of such systems may find them to be an irresistible expansion of their power, and if so, citizens' privacy may suffer. The end result of abuses of power is the threat that widespread use of video cameras may change the character, feel, and quality of American life itself.[39] Abuses of power associated with the use of video systems and databases may not be confined solely to "powers of authority," private citizens in possession of such technology may also use the technology to invade an individual's privacy and access personal information about that person. A later section of this article will discuss such abuses in the context of video voyeurism and reality filming.[40]

One problem with online databases is that they can be accessed by hackers and thieves, with resulting breaches in privacy to individuals and database owners. For example, the Federal Trade Commission recently required that data warehouser ChoicePoint Inc. pay a fine to settle charges that its security and record-handling procedures violated consumers' privacy rights and federal laws.[41] ChoicePoint collects data on individuals, including Social Security numbers, real estate holdings and current

---

[39] *What's Wrong With Public Video Surveillance? Available at* http://aolsvc.weather.aol.com/main.adp?location=USNC0120 (last visited Jan. 26, 2006).

[40] *Infra* sections VI and VII.

[41] *FTC Hits ChoicePoint With a $15 Million Fine*, *available at* http://articles.news.aol.com/news/article.adp?id=20060126095809990009&_mpc=news%2e10%2e4&cid=403 (last visited Jan. 26, 2005).

and former addresses. It has about 19 billion records, and its customers include insurance companies, financial institutions and federal, state and local agencies.[42] Choicepoint revealed that its massive database of consumer information was accessed by thieves posing as small business customers. The Federal Trade Commission said it fined the company ten million dollars, the biggest fine the agency had ever imposed, and that Choicepoint would be required to pay an additional five million dollars to compensate consumers.[43] The Federal Trade Commission indicated that "The message to ChoicePoint and others should be clear: Consumers' private data must be protected from thieves."[44] The settlement requires ChoicePoint to implement new procedures to ensure that it provides consumer reports only to legitimate businesses for lawful purposes, to establish and maintain a comprehensive information security program and to obtain audits by an independent third-party security professional every other year until 2026.[45] This example illustrates the difficulty of keeping an online database secure, and that information that is highly private and sensitive may be accessed by hackers and thieves, and may ultimately end up for sale to the highest bidder.

Another concern associated with video-based wearable computers and databases relates to an aspect of human nature. As video camera systems are operated by persons, they bring to the technology all their existing prejudices and biases. In Great Britain, for example, camera operators have been found to focus disproportionately on people of color, and the mostly male operators frequently focus voyeuristically on women.[46] Even

---

[42] *Id.*
[43] *Id.*
[44] *Id*.
[45] *Id.*
[46] *Electronic Privacy Information Center*, *available at* http://www.epic.org/privacy/surveillance/ (last visited Jan. 26, 2006).

though video surveillance by the police isn't as widespread in the U.S., as Great Britain, an investigation by the Detroit Free Press still shows the kind of abuses that can happen.[47] Looking at how a database available to Michigan law enforcement was used, the newspaper found that officers had used it to help their friends or themselves stalk women, threaten motorists, track estranged spouses - even to intimidate political opponents.[48] According to one commentator, the unavoidable conclusion is that the more people who have access to a database, the more likely that there will be abuse.[49] Facial recognition technology is especially subject to abuse because it can be used in a passive way that doesn't require the knowledge, consent, or participation of the subject[50] and once an image is an a database, it can be used in a way that far exceeds the original purpose of creating the database. According to one commentator, the creation of a database multiples the effects of sensors.[51] For example, video cameras have a far less intrusive effect on privacy if their only use is to be monitored in real time by a person. However, the longer the tapes are archived the greater their potential effect, and the more the tapes can be indexed according to who and what they show rather than just where and when they were made.[52] Further, the greater the amount of information about an individual that is placed in a database, the greater the danger that personal information and facts about the person may appear with the person's image on the internet resulting in a level of intrusion into

---

[47] M. L. Elrick, *Cops Tap Database to Harass, Intimidate,* DETROIT FREE PRESS, Misuse Among Police Frequent, Say Some, but Punishments Rare, July 31, 2001, *available at* http://www.sweetliberty.org/issues/privacy/lein1.htm (last visited Jan. 26, 2006).
[48] *Id*.
[49] *Id*.
[50] *Id*.
[51] A. Michael Froomkin, *The Death of Privacy*? 52 Stan. L. Rev. 1461 (2000).
[52] *Id*.

the private affairs of an individual, unknown before recent times.[53]

SOUSVEILLENCE

In response to the use of video cameras by authority figures to place individuals under surveillance or to film a person as they move around public spaces, is the idea that individuals may protect their privacy by "filming the filmers."[54] The term "sousveillance"[55] refers both to the concept of inverse surveillance (filming the filmers), as well as to the recording of an activity from the perspective of a participant in the activity.[56] An example of the latter idea is the use of phone cameras for what some have termed "citizen journalism."[57] On this point, consider George Holiday's videotape of Los Angeles police officers beating of Rodney King.[58] Another illustration of the recording of an activity from the individual's perspective comes from recent news headlines. After the terrorists bombing of the London subway which occurred July 21, 2005 some of the first video from the scene was from subway riders who filmed the scene with their phone cameras.

---

[53] The Total Information Awareness (TIA) program was a government program designed to mine data in commercial as well as government databases to spot patterns that could indicate terrorist activity. Hiawatha Bray, *Mining Data to Fight Terror Stirs Privacy Fears*, BOSTON GLOBE, Apr. 3, 2003, at C2, *available at* 2003 WL 3388980. Although Congress eliminated funding for TIA, similar efforts continue, *see* Duane D. Stanford, *ACLU Attacks Matrix on Privacy*, *available at* http://www.ajc.com/metro/content/metro/1003/31matrix.html (last visited Jan. 31, 2006) (describing an initiative by several state governments to develop a program similar to TIA, the Multistate Anti-Terrorism Information Exchange (Matrix)), *available at* 2003 WL 66525863.

[54] *See generally* Mann, *supra* note 25; Howard Kleinberg, *Video Cameras Turn the Tables on Big Brother*, L.A. DAILY J., Mar. 22, 1991, at 6 (claiming that we are a society that has become accustomed to instant replay).

[55] Mann, *id,* sousveillance is derived from inverse surveillance, taken from the French "sous" for "below", plus "veiller" for "to watch."

[56] *Id.*

[57] Paul J. Gough & Chris Marlowe, *Cell Phone Video First from London Bombing Scene*, WEB/NEW MEDIA: News, July 8, 2005, *available at* http://www.hollywoodreporter.com/thr/new_media/article_display.jsp?vnu_content_id=1000975698 (last visited Jan. 6, 2006).

[58] Katherine Fulton, *The Anxious Journey of a Technophobe*, Columbia Journalism Review, *available at* http://archives.cjr.org/year/93/6/technophobe.asp (last visited Jan. 28, 2006); *see also* Rodney King and the Los Angeles Riots, *available at* http://www.citivu.com/ktla/sc-ch1b.html (last visited Jan 26, 2006).

From the community that advocates "shooting back," as a response to video surveillance, has come the term "inverse surveillance" which is used to refer to the recording or monitoring of a real or apparent authority figure by others, particularly those who are generally the subject of surveillance.[59] Inverse surveillance is therefore considered a type of sousveillance.[60] According to Professor Mann, an example of inverse surveillance in the auditory domain occurs when one or more parties to a conversation record it, which represents an act of sousveillance; whereas when the conversation is recorded by a person who is not a party to the conversation, such a recording may be termed "surveillance."[61] Audio sousveillance is allowed in most states,[62] and by Federal law[63] but audio surveillance is illegal in most states.[64]

Some commentators argue that sousveillance, to some extent, reduces or eliminates the need for surveillance.[65] They argue that in this sense it is possible to replace the Panoptic God's eye view of surveillance with a more community-building ubiquitous personal experience capture.[66] In their view, crimes, for example, might be solved by way of collaboration among the citizenry equipped with video cameras rather than through the watching over the citizenry from above.[67] However, even with the

---

[59] Steve Mann, who coined the term souesveillance, describes it as "watchful vigilance from underneath." In contrast, surveillance denotes the "eye-in-the-sky" watching from above; whereas sousveillance denotes bringing the camera or other means of observation down to the human level, *see* Mann, *supra* note 25.

[60] "Hierarchical sousveillance" refers, for example, to citizens photographing police, shoppers photographing shopkeepers, or taxicab passengers photographing cab drivers, *see generally* Mann, *supra* note 25

[61] *Id.* at 635.

[62] *Id*. at 635-636. *See infra,* note 262.

[63] *See generally Advanced Electronics Group, Inc., available at* http://www.aegi.com/faqs.html (last visited Jan. 26, 2005).

[64] *Id.* Mann*, supra* note 25*; see generally* Antonietta Vitale*, Video Voyuerism and the Right to Privacy: The Time For Federal Legislation is Now*, 27 Seton Hall Legis. J. 381, 390-392 (2003).

[65] Mann*, supra* note 25.

[66] *Id.* at 634-637.

[67] *Id.* at 634-637.

proposed benefits of filming those that place individual citizens under surveillance, comes the risk of invading the privacy of other individuals not expecting to be filmed, this raises the fundamental questions of whether those engaged in sousveillance are simply replacing one filmer with another and whether by advocating the wearing of video cameras for the citizenry, we are building a society where every action by every individual is filmed- creating a society with zero privacy.

III. FACIAL RECOGNITION BIOMETRICS

As the focus of this article is on privacy in public places as a function of facial recognition software integrated into wearable computers, this section presents an overview of facial recognition technology. Facial recognition systems are computer programs that analyze images of human faces for the purpose of identifying them.[68] Generally, the facial scans captured by video are converted into numerical codes that are then stored and searched in databases.[69] Facial recognition programs work by recording a facial image, measuring facial characteristics, or landmarks, such as the distance between the eyes, the length of the nose, and the angle of the jaw, and then creating a file called either a "template" or "faceprint"[70] Some facial software systems define these landmarks as nodal points,[71] and there are about 80 nodal points on a human face.[72] These nodal

---

[68] A. Linney & A. M. Coombes, *Computer Modelling of Facial Form*, in Craniofacial Identification in Forensic Medicine, J. G. Clement & D. L. Ranson (eds.) (Arnold, London, 1998).

[69] I. Bajnoczky & L. Kiralyfalvi, *A New Approach to Computer-Aided Comparison of Skull and Photograph*, 108 International Journal of Legal Medicine 157-161 (1995); T. Catterick, Facial Measurements as an Aid to Recognition, 56 Forensic Science International 23-27 (1992); M. Y. Iscan *Introduction to Techniques for Photographic Comparison: Potential and Problems*, in Forensic Analysis of the Skull, M. Y. Iscan & R. P. Helmer (eds.) (Wiley, New York, 1993).

[70] W. R. Maples & D. E. Austin, *Photo/Video Superimposition in Individual Identification of the Living*, Presented at the 44th Annual Meeting of American Academy of Forensic Sciences, New Orleans, Louisiana, February 17–22 (1992); *see also* M. Proesmans & L. Van Gool, *Getting Facial Features and Gestures in 3D*, in Face Recognition, H. Wechsler, P. Jonathin Phillips, Vicki Bruce, Francoise Fogelman Soulie & Thomas S. Huang, eds., 288–309 (Springer, Berlin, 1998).

[71] Emelie Rutherford, *Facial-Recognition Tech has People Pegged*, *available at* http://archives.cnn.com/2001/TECH/ptech/07/17/face.time.idg/ (last visited Jan. 26, 2006).

points are measured by facial recognition systems to create a numerical code, a string of numbers that represents the face in a database.[73] Using templates, the software then compares a recorded image with a stored image and produces a score that measures how similar the images are to each other. Typical sources of images for use in facial recognition systems include video camera images and pre-existing photos such as those in driver's license databases.

The FaceIt facial recognition system which is a commercially available software package used to capture and compare facial images, will be used as an exemplar to describe how facial recognition systems operate in the field.[74] When FaceIt is attached to a video system, it searches the camera's field of view for faces. An algorithm is used to search for faces in low resolution.[75] If there is a face in the view, it is detected within a fraction of a second. The system switches to a high-resolution search only after a head-like shape is detected. A process termed "alignment" occurs once a face is detected and the system determines the head's position, size and pose. A face needs to be turned at some angle toward the camera, at least within 35 degrees for the version of FaceIt discussed here, in order for the facial recognition system to register it. The process of normalization occurs when the image of the head is scaled and rotated so that it can be registered and mapped into an appropriate size and pose.[76]

---

[72] *Id*.
[73] *Id.*
[74] FaceIt® is a scalable off-the-shelf facial recognition system that detects and identifies humans as they pass through a camera's field of view, *available at* http://www.identix.com/products/pro_security_bnp_argus.html (last visited Jan. 28, 2006).
[75] An algorithm is a program that provides a set of instructions to accomplish a specific task.
[76] Normalization is performed on the image regardless of the head's location and distance from the camera.

The heart of the FaceIt facial recognition system is the "local feature analysis algorithm."[77] The algorithm represents the mathematical technique used by the system to encode faces. The system maps the face and creates a faceprint, a unique numerical code for that face. Once the system has stored a faceprint, it can compare it to the thousands or millions of images stored in a database. According to one source, a facial recognition system can match multiple images at a rate of 60 million per minute from memory or 15 million per minute from hard disk.[78] As comparisons are made, the system assigns a value to the comparison using a scale of one to 10; if a score is above a predetermined threshold, a match is declared.

There are ongoing attempts to improve the accuracy of facial recognition techniques.[79] A recent advance in facial recognition systems is the use of the texture of the skin to assist in identifying an individual.[80] For example, using an algorithm called surface texture analysis, the surface of the skin can be analyzed for random features which results in a "skinprint," or skin template.[81] The skinprint can be used on its own to recognize faces, or can be fused together with traditional facial or fingerprint biometric techniques to increase the level of accuracy with current facial recognition systems.[82]

---

[77] FaceIt, *supra* note 74.
[78] *Disneys Technology*, *available at* http://www.lecs.cs.ucla.edu/site-specifics/index.php/Disneys_Technology (last visited Jan. 26, 2006).
[79] *Id.*
[80] *Facial Biometrics*, FaceIt's webpage, *available at* http://www.identix.com/trends/face.html (last visited Jan. 14, 2006). *See also Face-Off* (discussing the accuracy of various facial recognition systems), *available at* http://www.fcw.com/print.asp (last visited Feb. 1, 2006).
[81] *Id*.
[82] *Id*.

LIMITATIONS OF FACIAL RECOGNITION SYSTEMS

It has been reported by some commentators that there are severe limitations associated with facial recognition systems which itself brings up a host of legal issues.[83] For example, inaccuracies in facial recognition systems may result in misidentification of individuals or inaccurate or misleading information paired to a person's picture posted on the internet. One difficulty for facial recognition systems in that faces are highly complex patterns that often differ in only subtle ways, and it is very difficult for a machine-based system to match images when there are differences in lighting, camera, or camera angle between recorded and stored images.[84] There are also changes in the appearance of the face itself that make identification of individuals difficult, that is, unlike our fingerprints or irises, our faces do not stay the same over time. And facial recognition systems are easily influenced by changes in hairstyle, facial hair, or body weight, by simple disguises, and by the effects of aging.[85]

A study by the government's National Institute of Standards and Technology (NIST) found false-negative rates for face-recognition verification of 43 percent using photos of subjects taken just 18 months earlier.[86] The NIST study also found that a change of 45 degrees in the camera angle rendered the software useless.[87] Studies by

---

[83] Warned Julian Ashbourn, who wrote a book on biometrics called "*Biometrics: Advanced Identity Verification: The Complete Guide*" (Springer 2000), "There are a number of variables to the real-life application of facial technology, it will never be 100 percent accurate." *Id*. Because of these limitations, many companies using facial recognition software rely on a back-up or secondary system to verify results. *Id*.

[84] *Id.*

[85] *Id*.

[86] *Commerce's NIST Reports Significant Advances Made in Facial Recognition Technology*, *available at* http://www.nist.gov/public_affairs/releases/n03-04.htm (last visited Feb 1, 2006); *see also* 2002 Army Research Lab Study of Facial Recognition, link *available at* http://www.aclu.org/privacy/spying/15198res20030902.html (last visited Feb. 1, 2006*); Facial Recognition Systems: New Accuracy Study*, *available at* http://talkleft.com/new_archives/002184.html (last visited Feb. 1, 2006).

[87] *Id*.

NIST have shown that there are significant differences in facial matching abilities of facial recognition systems, depending on whether the images were taken indoors or outdoors.[88] It has been reported that facial recognition performance for outdoor images is only about half as good as for indoor images, where there is better control of lighting conditions.[89]

Generally, facial recognition technology works best under tightly controlled conditions, e.g., when the subject is staring directly into the camera under bright lights. Grainy, dated video surveillance photographs of the type likely to be on file for many individuals would be a poor template as a matching image. In addition, questions have been raised about how well the software works on dark-skinned individuals, whose features may not appear clearly on lenses optimized for light-skinned people. And finally, differences in facial expressions, such as when an individual yawns, may affect the accuracy of facial recognition systems.

IV. FACIAL RECOGNITION VIDEO SYSTEMS IN USE

The need to know the specific identity of an individual is a recent development in video surveillance and wearable computers and has led to the implementation of facial recognition software in systems with video capabilities. There are many current uses of facial recognition technologies coupled with wearable computers. For example, security personnel in major U.S. airports may use wearable computers equipped with facial recognition software so they can identify suspicious travelers.[90] The goal of a wearable

---

[88] *See* Philip Bulman, *Commerce's NIST Reports Significant Advances Made in Facial Recognition Technology*, *available at* http://www.nist.gov/public_affairs/releases/n03-04.htm (last visited Feb. 3, 2006).

[89] *Id.*

[90] Ramon G. McLeod, PCWorld.com, *Airport Security Adopts Wearable Computers*, *available at* http://pcworld.about.com/news/Nov132001id70826.htm (last visited Jan. 24, 2006).

computer security system is to get local verification' of an individuals identity so that the appropriate people at the terminal can get the information they need rapidly. Another application of wearable computers equipped with facial recognition software is the "iCare Interaction Assistant," a device for helping individuals who are visually impaired.[91] With this system, facial recognition technology is used as a social interaction assistant to help identify and interpret facial expressions, emotions and gestures and then communicate that information to visually impaired individuals.[92]

After the terrorist's attacks of 9-11,[93] the U.S. government has been actively investigating the use of biometric technologies[94] including facial recognition software that can potentially pick a suspected terrorist out of a crowded room.[95] Through this research agenda, the Department of Defense has been providing research funds to universities, with the goal of identifying people in a variety of lighting and background situations.[96] The goal of one such research project, HumanID,[97] is to develop automated

---

[91] Sreekar Krishna, Greg Little, John Black & Sethuraman Panchanathan, *Assistive Technologies for Individuals with Visual Impairments*, Proceedings of the 7th International ACM SIGACCESS Conference on Computers and Accessibility 106-113 (2005).

[92] *Id.*

[93] James Loy, U.S. Urges OSCE States to Adopt Biometric, Cargo Standards at OSCE Vienna Conference. "The United States shares lengthy and friendly borders with two countries… across which more than 500 million people, 130 million motor vehicles, and 2.5 million rail cars pass every year. But we also patrol nearly 95,000 miles of shoreline and waters, and more than 360 ports that see 8,000 foreign flag vessels, 9 million containers of cargo, and nearly 200 million passengers every year as well. Not to mention more than 500 airports that handle more than 30,000 flights and 1.8 million passengers every single day. In short, our borders are active places- where the engines of world commerce churn and the cameras of world tourists click," *Id*., *available at* http://usinfo.state.gov/gi/Archive/2004/Jun/24-993135.html (last visited Jan. 26, 2006).

[94] Biometrics refers to advanced identity verification techniques that use personal characteristics such as fingerprints, facial patterns, and so forth to identify individuals. These features of the technology cause some to raise the cry of Big Brother.

[95] Lucas Mast, *Biometrice: Hold On, Chicken Little, Issue #31*, *available at* http://www.cato.org/tech/tk/020118-tk.html (last visited Jan. 26, 2006).

[96] *See e.g*., I. Pavlidis & P. Symosek, *The Imaging Issue in an Automatic Face/Disguise Detection System*, Proceedings 2000 IEEE Workshop on Computer Vision Beyond the Visible Spectrum: Methods and Applications, 15-24, Hilton Head Island, South Carolina (2000).

[97] One aspect of the research project is to investigate Ther*mal Facial Screening* which is a non-invasive facial screening device that can detect psychological state (e.g. anxiety, alertness, and fear). Thermal

biometric identification technologies to detect, recognize and identify humans at great distances.[98] The federally funded research is also aimed at developing the capability to identify individuals based on their gait.[99]

Unlike other biometric systems, facial recognition can be used for general surveillance, usually in combination with public video cameras. There have been several such uses of facial recognition software in the United States thus far. One example is in airports, where video systems with facial recognition capabilities have been adopted in the wake of the terrorist attacks of 9-11.[100] And in some U.S. cities, such as Virginia Beach, Virginia, facial recognition technology has been implemented on public streets to search for criminals.[101] In addition, in England, where public, police-operated video cameras are widespread, individual towns such as Newham and London have experimented extensively with the technology.[102]

Most people are not aware of the pervasiveness and technological capabilities of video systems coupled with facial recognition software.[103] A recent field test of video-

---

facial detection and recognition operates in the near infrared band, the objective of which is a system that will detect faces of pedestrians and vehicle occupants under challenging illumination and weather conditions. *See also* Gait Detection Research at the Georgia Institute of Technology where researchers are developing technologies to recognize a person's walk, or gait, *available at* http://gtresearchnews.gatech.edu/newsrelease/GAIT.htm (last visited Jan. 28, 2006).

[98] Human ID at a Distance (HumanID), Program Manager: Jonathan Phillips, *available at* http://www.21cmagazine.com/issue2/iao_remix/humanid.html (last visited Jan.. 29, 2005).

[99] *Id*.

[100] Charlie Goodyear, SAN FRANCISCO CHRONICLE (December 17, 2001). Some argue facial recognition at Fresno's airport is too nosy. Since it began operating the system has falsely identified several passengers as potential suspects, according to airport officials, while registering no true matches. *Id*. Those passengers mistakenly identified were pulled out of line and questioned briefly before being allowed to pass, said Fresno airport spokeswoman Patty Miller. *Id*. *available at* http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2001/12/17/MN164532.DTL (last visited Jan, 26, 2006).

[101] *See Face Recognition, available at* http://www.epic.org/privacy/facerecognotion/ (last visited Feb. 1, 2006).

[102] *A History of Video Surveillance in England*, *available at* http://www.notbored.org/england-history.html (last visited Jan. 26, 2006).

[103] Laurent Belsie, *The Eyes Have it For Now*, Britain has an estimated 1.5 million surveillance cameras (some reports suggest 2.5 million or more), *available at* http://www.csmonitor.com/2002/1107/p15s02-lihc.html (last visited Jan. 26, 2006). No one knows how many surveillance cameras sweep public space

based surveillance highlights some of the capabilities and uses of video systems as applied to the general public. In January 2001, roughly 100,000 ticket-holders viewed the Super Bowl in Tampa, Florida. Secretly the police took pictures of every attendee as they entered the stadium through the turnstiles and compared the recorded photographic images against a database of some undisclosed kind; the recorded images were then compared to the database using facial recognition software.[104] The authorities would not say who was in that database, but the facial recognition software was reported to flag 19 individuals.[105] The police indicated that some of those were false alarms, and no one flagged by the system was anything more than a petty criminal such as a ticket scalper.[106]

Facial recognition systems are also being tested and used at public schools.[107] For example, in Phoenix, Arizona, facial recognition technology designed to recognize registered sex offenders and missing children has been installed at a school in a pilot project.[108] The video system installed at the school is linked to state and national databases of sex offenders, missing children and alleged abductors.[109] Using a wide-area network, video images captured at the school are transferred to the local Sheriff's office,

---

in the United States, but the number is rising. In Times Square, perhaps the nation's most monitored public area, the number of surveillance cameras more than tripled in a four year period. *Id.*

[104] Barbara Dority, *A Brave New World--Or a Technological Nightmare? Big Brother is Watching*! Humanist (2001).

[105] *Id.*

[106] *Id*.

[107] *School Face Scanner to Search for Sex Offenders: Civil Rights Groups Raise Concerns* (2003), *available at* http://www.cnn.com/2003/EDUCATION/12/12/facial.recognition.ap/ (last visited Jan. 28, 2006).

[108] *Id*.

[109] Justin Brown, *Maricopa County Tests Facial Recognition Technology in Schools*, Royal Palm Middle School is the first school nationwide to install cameras to detect faces of suspected child abductors, sex offenders or missing children, and instantly alert police. *Id.* If the pilot is successful, the Maricopa County Sheriff's Office hopes to expand the program to all 800 schools in the county. *Id*. (2004). *See e.g*., http://www.centerdigitaled.com/converge/?pg=magstory&id=90422 (last visited Jan. 28, 2006).

where facial recognition software[110] is used to scan 28 facial features of the recorded images in an effort to match them against images in databases containing missing children, suspected child abductors and sexual predators. Supposedly, images not matching the databases are immediately erased;[111] however, the ability to recover images erased from a computer hard drive, is a well-known technology and thus the storage of facial images in any database as the public exercises their right to move freely within public spaces is troublesome.

One of the most innovative uses of facial recognition is being employed by the Mexican government, which is using the technology to weed out duplicate voter registrations.[112] To sway an election, people will register several times under different names so they can vote more than once. Using facial recognition technology, officials can search through facial images in the voter database for duplicates at the time of registration.[113] New images are compared to the records already on file to catch those who attempt to register under aliases. The technology was used in the country's 2000 presidential election and is expected to be used in local elections as well.[114] Other current uses for facial recognition software is by casinos; law enforcement to digitalize mug shots; welfare departments to look for double-dippers; drivers' license bureaus to reduce

---

[110] One example is the Hummingbird facial recognition software, *see e.g.*, http://www.govtech.net/magazine/story.php?id=89806&issue=4:2004 (last visited Jan. 28, 2006).

[111] Brown, *supra* note 109. Civil libertarians have raised red flags about the idea, pointing to potential privacy violations, and biometrics experts say facial recognition programs are not foolproof.

[112] Cédric Laurant, *Privacy and Human Rights 2004, An International Survey of Privacy Laws and Developments, Electronic Privacy Information Center,* Washington, DC – USA. Mexican Government Adopts FaceIt® Face Recognition Technology to Eliminate Duplicate Voter Registrations in Upcoming Presidential Election, *available at* http://www.shareholder.com/identix/ReleaseDetail.cfm?ReleaseID=53264 (last visited Jan. 26, 2006).

[113] *Id*.

[114] *Id*.

I.D. forgers; and ATMs to separate clients from thieves.[115] Finally, a biometric security plan being tested by NASA, would also allow engineers to control unmanned spacecraft from their home computer, using both facial scanning and fingerprint readers.[116]

V. PRIVACY IN THE AGE OF WEARABLE COMPUTERS

As noted, wearable computers equipped with video-based facial recognition technology can be used to record and analyze a person's face, track their movements, and upload their image to the internet where personal information about the individual can be paired to the recorded image; does such a use of the technology result in an invasion of privacy under the current law?[117] To answer this question, the article first discusses the general concept of privacy, reviews Fourth Amendment law on search and seizure, and presents case law relating to the filming of individuals in a public place.

Samuel Warren and Louis Brandeis were the first legal scholars to introduce a comprehensive notion of a common-law right of privacy into American jurisprudence.[118] However, although they were the first legal scholars to document a right of privacy, privacy-related notions such as trespass, protecting property from invasion, and individual protections in criminal law already existed as integral parts of early American

---

[115] San Francisco's InnoVentry (which is going out of business), was using face-scanning software in its check-cashing machines to separate customers from crooks. The machines were designed to cater to check cashers who didn't have enough money to open a bank account. A camera incorporated into InnoVentry's machines was used to scan customers' faces when they tried to cash a check for the first time. The image was then compared with a "negative file" of people who had tried to pass bad checks. If no matches were made, the customer completed the transaction. On the next visit, all the customer had to do to get the cash was type in the correct social security number and get his or her face scanned. *Id*. *Available at* http://www.atmmarketplace.com/news_story_10825.htm (last visited Jan. 29, 2006).

[116] Julina Scheeres*, Smile, You're On Scan Camera*; and Declan McCullagh, *Call it Face Scan I*, both *available at* http://www.mckinnonsc.vic.edu.au/la/it/ipmnotes/biometrics/facescan.htm (last visited Jan. 28, 2006).

[117] Consider that in Anchorage Alaska, at one time video images from surveillance cameras were not transferred to the police department, but instead were sent to resident's home computers. 20/20: The Eyes of the Law (ABC television broadcast, Sept. 8, 1995, transcript 1536) at 6.

[118] Warren & Brandeis, *supra* note 19 at 193.

law.[119] *Warren and Brandeis* defined privacy as a right to "be let alone"[120] and centered their concern upon technological devices that existed in the 1890's, especially "instantaneous" photographs.[121] In calling for new law to remedy invasions into people's privacy, *Warren and Brandeis* argued that "political, social, and economic" changes in society required recognition of new rights and that the common law should adapt to accommodate those societal needs.[122] Now days, the development of wirelessly networked wearable computers equipped with miniature cameras, may pose an equal if not greater challenge to an individual's right to privacy as did the use of still photographs in the 1890's. While in either case, an individual may be exposing their image to the scrutiny of the general public when they enter a public place- the scope of the exposure, the extended length of time an individual's image may be recorded, the almost instantaneous nature of posting the recorded image on the internet, the ability of software to analyze the individual's image, and the ability of software to search databases and provide personal information about an individual- all represent a significant advance in the ability of technology to invade a persons "right to be left alone" once they enter a public place.

Interestingly, the United States Constitution contains no direct reference to a right of privacy; but the High Court has held that such a fundamental right does exist. In *Griswold v. Connecticut*, the United States Supreme Court stated that privacy was a fundamental right established through the "zone of privacy" found within the Bill of

---

[119] *See generally* Turkington, *supra* note 19.
[120] Warren & Brandeis, *supra* note 19, at 193.
[121] *Id*. at 195.
[122] *Id.* at 193.

Rights.[123] Despite this concept of privacy, an individual's right under the Constitution to protect themselves from interested observers remains limited. In fact, early courts initially declined to recognize the "right to be left alone" as expressed by *Warren and Brandeis.*[124] For example, in *Roberson v. Rochester Folding Box Co.*, the New York Court of Appeals dismissed a suit for invasion of privacy by a woman whose picture was placed on 25,000 poster's advertising defendant's flour without her consent.[125] The court failed to provide relief and declared that no right to privacy existed.[126] In response to the public outcry after *Roberson*, the New York legislature enacted section 51 of the Civil Rights Law providing a cause of action for anyone whose name, portrait or picture was used for advertising or for purposes of trade without written consent.[127] A few years after the *Roberson* case was decided, the Supreme Court of Georgia in *Pavesich v. New England Life Insurance Company*, recognized a common law right to privacy where the defendant published the plaintiff's name and picture to advertise its insurance services without the plaintiff's consent.[128] In the 1930s, most jurisdictions accepted a common-

---

[123] *Griswold v. Connecticut,* 381 U.S. 479, 485-486 (1965) (the Court held a Connecticut statute unconstitutional for violating the privacy rights of married people). The statute criminalized the use of any contraceptive. *Id*. at 480. In a five-four decision, Justice Douglas, writing for the majority, reasoned that the Bill of Rights created a penumbra of privacy rights that establish a zone of privacy for all persons protected by the Constitution. *Id*. at 484. In particular, Justice Douglas cited to the Court's holding in *Mapp v. Ohio*, 367 U.S. 643 (1961), which referred to the Fourth Amendment as creating a "right to privacy, no less important than any other right carefully and particularly reserved to the people." *Id*. at 485.

[124] Warren & Brandeis, *supra* note 19.

[125] *Roberson v. Rochester Folding Box Co.*, 64 N.E. 442 (1902).

[126] *Id*.

[127] New York Civil Rights Law, Sec. 50. Right of Privacy. "A person, firm or corporation that uses for advertising purposes, or for the purposes of trade, the name, portrait or picture of any living person without having first obtained the written consent of such person, or if a minor of his or her parent or guardian, is guilty of a misdemeanor." *Id.*

[128] *Pavesich v. New England Life Insurance Company,* 50 S.E. 68 (1905).

law right of privacy, and the first Restatement of Torts recognized this common-law right in 1939.[129]

More recently, Professor Lawrence Tribe described the essence of an individual's right to privacy, the "right to be left alone," as "nothing less than society's limiting principle . . . . It is a right which has meaning only within the social environment from which it would provide some degree of escape."[130] In 1960, Dean William Prosser authored a seminal article on privacy that compiled a mixture of privacy tort cases decided since the publication of the *Warren and Brandeis* article.[131] In his influential article, Prosser argued that the invasion of privacy tort, designed by *Warren and Brandeis*, was actually comprised of four distinct categories of tort privacy.[132] Prosser labeled these torts as intrusion upon seclusion, public disclosure of private facts, false light, and appropriation.[133] Drafters of the Restatement (Second) of Torts subsequently incorporated Prosser's four privacy tort definitions into the Restatement's privacy sections.[134] Courts in most states have recognized Prosser's privacy torts, and many courts have adopted language directly from the Restatement sections.[135] In several jurisdictions, courts have accepted the three privacy torts of intrusion upon seclusion, public disclosure of private facts, and appropriation; however, some courts have excluded

---

[129] Restatement (First) of Torts (1939).

[130] *See generally* Lawrence Tribe, *American Constitutional Law*, 1302 (West Publishing Company, 2d ed. 1988). *See* William L. Prosser, Privacy, 48 Cal. L. Rev. 383, 386 (1960) (describing privacy torts recognized in 47 states); *see* W. Prosser, W. Page Keeton, Dan B. Dobbs, Robert K. Keeton & David G., Owen, *Prosser and Keeton on the Law of Torts* 849-869 (West Group 5th ed. 1984).

[131] Prosser, *id*.

[132] *See* Prosser, *id*. at 389 (establishing existence of four separate torts under privacy right).

[133] *See* Prosser, *id*. at 389 (listing four different privacy torts). The categories are described in the following way: intrusion upon the plaintiff's seclusion or solitude, or into his private affairs; public disclosure of embarrassing private facts about the plaintiff; publicity which places the plaintiff in a false light in the public eye; appropriation, for defendant's advantage, of the plaintiff's name or likeness.

[134] *See* McClurg, *supra* note 15, at 998 (discussing inclusion of four tort definitions into Restatement (Second) of Torts). *See* Restatement (Second) of Torts §§ 652A-652E (1976) (listing actionable privacy torts).

[135] *See* McClurg, *supra* note 15, at 1036.

the tort of false light.[136] Nearly every jurisdiction recognizes some form of a tortious right of privacy.[137]

Prosser's review of intrusion upon seclusion case law revealed a variety of cases, some allowing recovery for physical intrusion and others extending beyond physical intrusion.[138] According to Prosser, the privacy tort of intrusion overlapped with the torts of trespass and intentional infliction of emotional distress.[139] Further, *Prosser* derived two limiting factors from the case law that would separate tortious intrusion from non-tortious intrusions.[140] First, a reasonable person must find the intrusion offensive or objectionable;[141] second, the intrusion must be into something private in nature.[142] Under the second limiting factor, Prosser drew a strong distinction between protection in a private location and a lack of protection in public spaces.[143] The article explicitly stated that taking a photograph of a person in a public place or on a public street would not

---

[136] *See* McClurg, *supra* note 15, at 998 (listing jurisdictions that recognize intrusion, disclosure, and appropriation torts).

[137] *See* McClurg, *supra* note 15, at 998 (explaining that most jurisdictions have adopted some form of tort action protecting right of privacy).

[138] *See* Prosser, *supra* note 130, at 389-390 (summarizing cases of physical and non-physical intrusion). Physical intrusion cases include intrusion into a home, a hotel room, a woman's stateroom on a steamboat, and a shopping bag at a store. *See id*. at 389 (listing cases of physical intrusion). Non-physical intrusion cases include eavesdropping through wiretapping and microphones, peering into windows of homes, and prying into a bank account; *see id*. at 390 (listing cases of non-physical intrusion).

[139] *See* Prosser, *supra* note 130 at 389-390 (suggesting recognition of independent tort accomplishes same result).

[140] *See* Prosser, *supra* note 130, at 390-391 (discussing limiting factors).

[141] *See Gill v. Hearst Publishing Co., supra* note 36, at 227 (stating plaintiffs' allegation that republished photograph of pose invaded right of privacy). The plaintiffs actually filed two separate right of privacy claims based upon this photograph. *See* Prosser, *supra* note 130, at 407 (discussing two distinct right of privacy claims). In *Gill v. Curtis Publishing Co*. (Gill I), the plaintiffs asserted the publication of the photograph violated the plaintiffs' right of privacy by depicting the couple's pose as the "wrong" kind of love in a written caption appearing below the picture. *See Gill v. Curtis Publ'g Co.,* 38 Cal. 2d 273, 275, (1952) (reviewing plaintiffs' factual basis for their right of privacy claim). The Supreme Court of California decided the plaintiffs' complaint stated a cause of action under a right of privacy claim based on the publication of the photograph, which characterized the couple as "dissolute and immoral and robbed them of public esteem." Gill v. Curtis Publ'g Co., *id.* at 281. Prosser placed the claim in Gill I in the privacy tort law category of "false light in the public eye." Prosser, *supra* note 130, at 407 (categorizing Gill decisions into two separate privacy tort groups). Prosser classified *Gill v. Hearst Publishing Co.* (Gill II) in the category of public disclosure of private facts.

[142] *See* Prosser, *supra* note 130 at 391 (listing second limiting factor).

[143] *Id.* at 391 (discussing limitation of recovery in public setting).

qualify as actionable under the privacy tort of intrusion.[144] In an age of wirelessly networked wearable computers, would a court using the same principles as developed by Prosser conclude that an image recorded in a public place, analyzed, and uploaded to the internet was an invasion of privacy under the tort of intrusion? Clearly, since Prosser's seminal article was published, the ability of technology to invade a person's privacy has increased several fold, and in some cases the law on privacy has adapted to changes in technology as witnessed by state and federal statutes,[145] and state constitutions which include a right to privacy.[146] However, even with changes in the law designed to protect an individual's privacy under specific circumstances,[147] the law has not adequately changed to protect the privacy of individuals once they enter a public place in an age of wirelessly networked, video-based, wearable computers- especially given that such systems can be used to track an individuals movements and pair personal information about an individual to their image posted on the internet.

Of significance to video-based wearable computers, was Prosser's conclusion that there can be no intrusion of privacy in a public place; this conclusion rested on two premises:[148] (1) that a person effectively assumes a risk of scrutiny when entering a public place;[149] and (2) that there was no distinguishable difference between merely observing a person and taking their photograph. However, recent technology may have changed the premises under which Prosser concluded that an individual in a public place may not claim a right of privacy from intrusion. For example, related to the first premise,

---

[144] *See id*. at 391-392 (describing such as analogous public locations).
[145] *See* Advanced Electronics Group, Inc., *supra* note 63.
[146] *See infra* note 254.
[147] Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681; Drivers Privacy Protection Act, 18 U.S.C. § 2721 (1994).
[148] *See* McClurg, *supra* note 15, at 1036 (stating conclusion based on implicit and explicit premises).
[149] *See id*. (observing assumption of risk of public inspection as implicit premise).

given the ability of video-based wearable computers to record a person's image, search databases, and upload the person's image to the internet, a danger associated with networked wearable computers could be the pairing of inaccurate or highly personal information to an individual's image. Such a result could lead to a form of "digital scarlet letter" attached to the individual's image, accessible by millions on the internet. Regarding Prosser's second premise, video systems equipped with facial recognition software and wireless internet access will allow far more to be known about an individual than can be discerned by simply looking at a still photograph. That is, given the extensive information about each person that is searchable on the internet, including medical and financial records, phone records, biographical and family information, and employment histories, the potential to know far more than just what a person presents to the public when entering a public space is entirely possible once the person's identity is known.

In an early case, decided well before wirelessly networked video-based wearable computers were developed, the court in *Gill v. Hearst Publishing*[150] provided support for Prosser's conclusions regarding a lack of privacy in public places.[151] This privacy case arose when a photographer took a photograph of a couple in a romantic pose at the Farmers' Market in Los Angeles.[152] The couple asserted that the photograph published in a magazine without their consent violated their right of privacy.[153] The *Gill* court decided that the couple waived their right of privacy when they voluntarily assumed an amorous

---

[150] Gill v. Hearst Publ'g Co., 40 Cal.2d at 229.

[151] *Id*. at 441.

[152] *See* Prosser, *supra* note 130, at 391-392 (arguing photographs taken in public places merely record which is similar to written description). Prosser cited *Gill v. Hearst Publishing Co.* for the proposition that photographs taken in a public space do not intrude into a person's privacy.

[153] *See* Gill v. Hearst Publ'g Co., 40 Cal.2d 224. Photojournalist took a photograph of the plaintiffs at their place of work, a confectionery and ice cream concession in the Farmers' Market. The photo captures an image of a young man and woman seated with the man's arm around the woman while the woman focuses intently upon a notebook.

pose in a public setting.[154] Additionally, the court concluded that the photograph "did not disclose anything which until then had been private, but rather only extended knowledge of the particular incident to a somewhat larger public than had actually witnessed it at the time of occurrence."[155] Clearly the use of facial recognition software coupled with the ability of a computing system to search vast databases almost instantaneously, and to pair that information to a particular individual, goes far beyond the alleged invasion of privacy considered by the *Gill* court and thus can be distinguished from the facts presented in *Gill.* A court deciding whether an individual using a wearable computer equipped with facial recognition software violates an individual's privacy, may find the increased intrusiveness of a wirelessly networked wearable computer with facial recognition software actionable under tort law.

Prosser drew a similar distinction between public and private facts in his review of the second privacy tort of public disclosure of private facts.[156] The public disclosure of embarrassing private facts, similar to intrusion, requires intrusion into something that is secret, secluded, or private.[157] Additionally, the disclosure tort measures the matter made public using a reasonable person standard.[158] In the case of wearable computers, would a reasonable person expect when entering a public place that their image would be filmed and uploaded to the internet viewable by millions of people around the world? And

---

[154] Gill v. Hearst Publ'g Co., 40 Cal.2d 224.

[155] *See* Gill v. Hearst Publ'g Co, 40 Cal.2d 224 (concluding couple's romantic pose in public market place functioned as waiver of privacy right). The Supreme Court of California emphasized the voluntary nature of the plaintiffs' action in a public setting in its analysis showing that the pose, and the photograph, by extension, reveals a public fact and not a private fact. *Id.*

[156] Gill v. Hearst Publ'g Co, 40 Cal.2d 224 at 445.

[157] *See* Prosser, *supra* note 130, at 407 (explaining common feature between intrusion and disclosure privacy torts).

[158] *See* Prosser, *supra* note 130, at 396-397 (limiting scope of tort to published matters that seem offensive and objectionable to reasonable person).

would a reasonable person expect that their image posted on the internet without their consent would contain personal information?

On the issue of the reasonable person standard, in *Miller v. National Broadcasting Co*.,[159] the court held that a heart attack victim's wife could sue a local television news producer when a camera crew entered her bedroom along with paramedics. The court concluded that a valid cause of action existed against the television network and the news producer for invasion of privacy.[160] The court also concluded that reasonable people could see this intrusion as highly offensive.[161] However, in many cases, if the information disclosed is newsworthy, an individual claiming a right from intrusion onto secret, secluded, or private information would lose as the disclosure of private facts tort is balanced against the First Amendment's protection of freedom of the press using a "newsworthiness" test.[162] In such cases, Courts will often strike that balance in favor of the First Amendment's highly protected freedom of the press.[163] Therefore, to the extent that an individuals facial image captured and posted on the web by a wearable computer

---

[159] *Miller v. Nat'l Broad. Co*., 187 Cal.App.3d 1463, 1482-1487 (Cal. Ct. App. 1986).

[160] *See id*. at 678-681. Also, under *Lovell v. Griffin*, 303 U.S. 444, 452 (1938) the constitutional guaranty of expression applies equally to the publication of a news report as to an entertainment feature.

[161] Miller, 187 Cal.App.3d at 679.

[162] Geoff Dendy, *The Newsworthiness Defense to Public Disclosure T*ort, 85 Ky. L.J. 147, 151 (1997). *See* Ellen Alderman & Caroline Kennedy, *The Right to Privacy,* at 166 (Knopf 1995) (explaining use of "newsworthiness" test to strike balance between disclosure tort and First Amendment's free press rights). A plaintiff must prove that the private matter published was not a matter of "legitimate concern to the public" to win a public disclosure tort case. *Id*. The two main defenses to the invasion of privacy tort are consent and newsworthiness; "Consent is easily asserted where the plaintiff in the private facts suit had knowledge of the contents of the disclosure and acquiesced to its publication," while the definition of newsworthiness is subject to a variety of judicial interpretations. *Id.* Generally speaking, newsworthiness "amounts to a showing that the public has a legitimate interest in the disclosed fact, and, if established, precludes any recovery under the private facts tort." *Id.*

[163] *See* Alderman & Kennedy, *id*, at 166 (noting that satisfying "newsworthiness" test creates a high burden because courts have construed newsworthy broadly).

is newsworthy, the First Amendment may serve as a defense to the publication of the image.[164]

The first constitutional challenge of the private facts tort addressed by the Supreme Court was in *Cox Broadcasting Corp v. Cohn*.[165] Here the Court acknowledged the need for the right to privacy but noted that the private facts tort "most directly confronts the constitutional freedoms of speech and press."[166] Limiting its decision to the narrow issue at bar, the Court held that a state may publish a rape victim's identity obtained from judicial documents that are open to public inspection, provided the information is accurate.[167] By failing to address the broader question of whether the publication of truthful information could ever be punished, the Cox decision merely reaffirmed that the private facts tort addresses the disclosure of private, truthful facts.[168] In *Florida Star v. B.J.F.*, the Supreme Court invoked the First Amendment to find no liability for a newspaper who published the name of a rape victim received from a police department press release.[169] However, the Court expressly rejected the newspaper's broad claim that the press could never be held liable for publishing the truth.[170] As the *Cox* case was decided over 30 years ago, the issue a court may have to decide today is whether a rape victims identity, if paired to the facts of the rape, and posted on the internet by a person using a wirelessly networked wearable computer, would result in an invasion of the victim's privacy. If the court determines that the

---

[164] The court may also determine if the internet cite in which the image is posted constitutes a news publication.
[165] *Cox Broad. Corp. v. Cohn*, 420 U.S. 469 (1975).
[166] John A. Jurata, Jr., *The Tort That Refuses to Go Away: The Subtle Reemergence of Public Disclosure of Private Facts*, 36 S.D. L. Rev. 489, 494 (1999); Prosser, *supra* note 130, at 386-388 (quoting Cox, *id*. at 489).
[167] Jurata, *id*. at 499; *see also* Cox, *supra* note 165, at 491-496.
[168] Jurata, *id*. at 500.
[169] *Id*.; *see also Florida Star v. B.J.F.*, 491 U.S. 524 (1989).
[170] Jurata, *supra* note 167, at 501, *see also* Florida Star, *id.* at 532.

information was not newsworthy and consent was not given, it may conclude that under tort law the individuals privacy had been violated; however, the "newsworthy" test is a high bar for plaintiffs to overcome.

Prosser's third privacy tort consisted of publicity that placed a person in a false light.[171] The false light tort guards against an objectionable false portrayal of a person.[172] Prosser noted two typical false light circumstances: a publisher who uses a person's picture to illustrate a book or article when that person has no connection with the article, and a police department which includes a non-convicted person's name, photo, and fingerprints among a group of convicted criminals.[173] Prosser observed that the false light tort overlapped greatly with defamation.[174] Since a video-based wearable computer system may project false or inaccurate information about an individual, or distort the video image of a person posted on the internet, such a result may be actionable under the tort of placing a person in a false light. As discussed in the following sections of the article critical issues in defining whether a tort is actionable will be the consent or lack there of, provided by the individual whose image is captured by a wearable computer system; as well as the status of the person filmed in the public place.

---

[171] *See* Prosser, *supra* note 130, at 398-401 (discussing third form of privacy tort that protects person's reputation); *see also* Alderman & Kennedy, *supra* note 162, at 195-197 (comparing false light tort with defamation law).

[172] *See* Prosser, *supra* note 130, at 398-400 (explaining false light tort's purpose in protecting reputation interest). The false portrayal must also be objectionable under the reasonable person standard.

[173] *See* Prosser, *supra* note 130, at 399-400 (describing examples of previous false light torts).

[174] *See* Prosser, *supra* note 130, at 400 (observing significant overlap between false light tort and defamation requiring publication of false information); *see also* Alderman & Kennedy, *supra* note 162, at 195-197 (discussing different standards applied by states to distinguish between false light and defamation actions).

The fourth privacy tort, “appropriation,” prohibits the unlawful use of a person's name or identity for a defendant's benefit or advantage.[175] This fourth tort of invasion of privacy differs significantly from the other three torts because appropriation deals with a proprietary interest as opposed to a personal privacy interest.[176] This tort often assists celebrities in protecting the commercial value of their "right of publicity."[177] Of relevance for video-based wearable computers and privacy, the right of publicity cause of action was brought forth in a case involving the videotaping of a young woman whose image appeared in the video titled “Girls Gone Wild- College Girls Exposed.”[178] The facts of the case indicated that while on a public street, the plaintiff was encouraged by a videographer to remove her clothes and expose areas of her body.[179] Some time later, she discovered that two minutes of footage taken of her appeared in the “Girls Gone Wild- College Girls Exposed” video, and two to three seconds of censored clips of the plaintiff were being used in television commercials to advertise the videos.[180] The plaintiff brought suit under Florida's statutory version of the right of publicity, section 540.08.[181] Section 540.08 of the Florida Statute prohibits the unauthorized publication "for purposes of trade or for any commercial or advertising purpose the name, portrait, photograph or other likeness of any natural person without the express written or oral consent to such

---

[175] *See* Prosser, *supra* note 130, at 401-407 (discussing appropriation tort protecting against prohibited use of person's identity for third person's benefit).

[176] *See* Prosser, *supra* note 130, at 406 (contrasting proprietary protection of exclusive use of person's name or likeness with other three torts' protection of personal privacy).

[177] *See* Prosser, *supra* note 130, at 406-407 (explaining creation of "right of publicity" out of appropriation statute); *see also* Alderman & Kennedy, *supra* note 162, at 221-222 (detailing case examples when celebrities protected their "right of publicity").

[178] *Lane v. MRA Holdings*, 242 F.Supp.2d 1205 (MDFla. 2002).

[179] *Id.* at 1209.

[180] *Id*. at 1210.

[181] FLA. STAT. § 540.08 (West 2002) (providing "No person shall publish, print, display or otherwise publicly use for purposes of trade or for any commercial or advertising purpose the name, portrait, photograph or other likeness of any natural person without the express written or oral consent to such use given by . . . such person.").

use given by such person.[182] The defendant, argued its videos were expressive works, like motion pictures, aiming to entertain,[183] and that the documentaries showing real women in actual public places were entitled to First Amendment protection.[184] The court agreed and found the Girls Gone Wild video to be "irrefutably" an expressive work created solely to entertain.[185]

What the above discussion indicates is that there is presently no appropriate cause of action under tort law for an intrusion into a person's privacy when they enter a public place and their image is recorded, analyzed, and uploaded to the internet by an individual using a wearable computer. However, if broadly defined, the concept of information privacy may involve an individual's personal information and his ability to control that information; if so, then the above capabilities of wearable computers represents a significant means to violate the information privacy rights of an individual once they have entered a public place.

STATUS OF THE PERSON IN THE PUBLIC PLACE

When considering whether an individual's privacy in a public place is violated when their image is filmed by a wearable computer, uploaded to the internet, and paired to personal information about the individual, the status of the person filmed must be considered. The consideration of the status of the individual once they enter a public place is especially important if the defendant in a privacy suit relies on a "newsworthiness" defense. Generally, those who have achieved a marked reputation or

---

[182] FLA. STAT., *id.*
[182] *See id.*
[183] *See* Stephen Van Drake, *Girls Gone Wild' Cases Test Constitution*, *available at* http://washington.bizjournals.com/southflorida/stories/2002/08/12/story4.html (last visited Feb. 1, 2006).
[184] *Id.*
[185] Lane, 242 F.Supp.2d 1205.

notoriety by appearing before the public can expect that their accomplishments and way of life will be the subject of print, radio, or television attention.[186] Therefore, public figures have to some extent lost the right to privacy in public places and are thus subject to fair comment and criticism by the media.[187] In this regard, the Fifth Circuit has noted that one of the public interest privileges in reporting private facts is to report truthful facts concerning public figures.[188]

The Restatement holds that "one who voluntarily places himself in the public eye, by engaging in public activities, or by assuming a prominent role in institutions or activities having general economic, cultural, social or similar public interest, or by submitting himself or his work for public judgment, cannot complain when he is given publicity that he has sought, even though it may be unfavorable to him."[189] No right of privacy remains for the public figure in relation to his public activities and appearances since these are no longer private affairs.[190] However, while no cause of action exists regarding revelations involving the public figure relating to his famous status, liability may arise when the interest of the public exceeds the range of information that would otherwise be considered private.[191] In fact, one California court has held that public figures are entitled to keep some information about their domestic activities and sexual

---

[186] Gary Williams, On *the QT and Very Hush Hush: A Proposal to Extend California's Constitutional Right to Privacy to Protect Public Figures from Publication of Confidential Personal Information*, 19 Loy. L.A. Ent. L. Rev. 337, 347 (1999). *See Carlisle v. Fawcett Publ'n, Inc*., 201 Cal.App.2d 733, 745-746 (Cal. Ct. App. 1962); *see* 44 N.Y. Jur 2D Defamation and Privacy § 323 (2003) ("a person who, by his accomplishments, fame, or mode of life, or by adopting a profession or calling which gives the public a legitimate interest in his doings, his affairs, and his character, may be said to have become a public figure."); *see also* 62A AM. JUR. 2D Privacy § 193 (2002).

[187] *See Carlisle Fawcett Publications*, 20 Cal.App.2d 733. *See generally* 62A AM. JUR. 2d Privacy § 193 (2002); *Briscoe v. Readers' Digest Ass'n*, 483 P.2d 34 (Cal. 1971).

[188] *Campbell v. Seabury Press*, 614 F.2d 395, 397 (5th Cir. 1980).

[189] Restatement (Second) of Torts § 652D cmt. e (1977).

[190] *Id.*

[191] *Id*.

relations private.[192] Further, California's has an anti-paparazzi law that protects a public figures privacy against journalists who might engage in either physical or constructive trespasses to obtain images of, as the statute puts it, "personal or familial activities."[193] However, the statute does not seem applicable to the use of wirelessly networked wearable computers that are used to record an individual in a setting other than their home as it does not cover activities on public streets. The California law reveals a deficiency in privacy law as it exists today; while it may be permissible to film a public figure once they enter a public place, in some cases, the publication of personal information about the individual could result in liability. In the past such actions, the filming of an individual, and the publication of private facts about an individual occurred at separate times, therefore, the law could separate the two in regards to privacy, now with wearable computers, the recording and publication can occur almost simultaneously, yet no current law accounts for this capability.[194]

Two early cases that are often quoted have divergent views of the public figure's relation to the private facts tort. In *Melvin v. Reid*, the plaintiff was a former prostitute who had been acquitted of murder.[195] Subsequently, Melvin turned her life around and lived respectably in the private sector for many years in a community that had no

---

[192] *Diaz v. Oakland Tribune, Inc*., 139 Cal.App.3d 118 (Cal. Ct. App. 1983).

[193] Cal. Civ. Code 1708.8, California Anti-Paparazzi Legislation (2004). The law takes which took effect January 1, 2006, triples the amount of damages a celebrity can sue a photographer for, as well as making employers liable for the first time. Further, the photographers could also be required to disgorge any profits they make from the offending pictures. Robert D. Richards & Clay Calvert, *Suing the Media, Supporting the First Amendment: The Paradox of Neville Johnson and the Battle for Privacy*, 67 Alb. L. Rev. 1097, 1109 (2004).

[194] *See generally* Woodrow Barfield & Thomas Caudell (eds), *Fundamentals of Wearable Computers and Augmented Reality* (Lawrence Erlbaum Press, 1998). If the individual with the wearable computer is using an opaque visual display (*see* Mann *supra* note 25), then information from the wirelessly networked wearable computer can be projected into the real world and merged with physical objects. If only one person viewed the display, the court may conclude no cause of action, however, it is possible that several individuals with wearable computers could access the recorded image paired with personal facts if they had networked computers.

[195] *Melvin v. Reid*, 297 P. 91 (Cal. Ct. App. 1931).

knowledge of her past.[196] However, her history was revealed in a movie about the murder case that used her actual maiden name.[197] The court held that the creation of the movie violated her right to privacy because she had successfully reclaimed her private figure status.[198] The use of wearable computers with facial recognition capabilities could make it much more difficult for an individual to reclaim their private life once they had left the limelight as numerous "watching eyes" could be ever vigilant once they were programmed to search for particular individuals. However, in a case showing the law in this area is unsettled, the Second Circuit determined in *Sidis v. F-R Publishing Corp.*, that a reclusive former child prodigy who had hidden from the media for years was not a private figure.[199] Sidis sued The New Yorker magazine after he was featured and mocked in a "where is he now" article, but the court held that his public figure status had not diminished with the passing of time.[200] In contrast to the *Melvin* decision,[201] the Sidis decision seems to stand for the premise that at some point the public interest in obtaining information becomes dominant over the individual's desire for privacy.[202]

Involuntary public figures, are persons who have not sought public attention but who have become "news" as the result of their involvement in or association with an otherwise newsworthy event.[203] This category includes crime victims, accident victims, accused criminals, and people who perform heroic acts.[204] Additionally, those who are

---

[196] *Id*. at 91.
[197] *Id*. at 91.
[198] *Id*. at 93.
[199] *Sidis v. F-R Publishing Corp*., 113 F.2d 806, 809 (2d Cir. 1940).
[200] *Id*.
[201] Melvin, 297 P. 91.
[202] Sidas, 113 F.2d 806.
[203] Williams, *supra* note 186, at 348.
[204] *Id*.

related to voluntary public figures gain involuntary public figure status.[205] The Seventh Circuit opined that involuntary public figures have no legal right to regain their private status as long as the newsworthy events that made them public figures remain in the public interest.[206] The court noted that even if these people do not desire publicity and would prefer that their experiences remain private, they are not equipped with the legal means to do so.[207] However, in *Leverton v. Curtis Pub. Co*, the Third Circuit remarked that the invasion of privacy rights of involuntary public figures is not without limits.[208] The case concerned a young girl who had been involved in a car accident at age ten and had the misfortune of being photographed at that time.[209] At a later date, another magazine published the picture from the accident and the victim sued for invasion of privacy.[210] Although ultimately finding for the publishers, the court declared that the plaintiff's life may not be subjected to continuous public scrutiny and would only risk attention in situations closely related to the initial car accident.[211]

Another type of figure that may be found in a public place are private figures; this category represents the vast majority of people who could be filmed by a wearable computer once they entered a public place. While intuitively, private figures should have a greater expectation of privacy than public figures, most jurisdictions do not consider the status of the plaintiff in determining newsworthiness. The Supreme Court has stated, in dicta, that the risk of exposure to public view is an "essential incident of life in a society which places a primary value on freedom of speech and of press," so even private

---

[205] *Id*.
[206] *Haynes v. Alfred A. Knopf, Inc*., 8 F.3d 1222, 1232 (7th Cir. 1993).
[207] *Id*.
[208] *Leverton v. Curtis Pub. Co.*, 192 F.2d 974 (3d Cir. 1951).
[209] *Id.* at 974-975.
[210] *Id.* at 975.
[211] *Id*. at 976.

citizens' rights of privacy are difficult to protect.[212] Arguably, the tendency of the courts to favor the press over individuals, coupled with privacy-seeking people's reluctance to broadcast their private facts in court, has prevented the full development of the private facts tort.[213] To this end, when the plaintiff in a private facts tort is a private figure, the "right to be let alone" must still be balanced against the public interest in the dissemination of news and information, as well as the constitutional guarantees of freedom of speech and of the press.[214]

The right of privacy's main objective is to protect private life, and it is determined by a reasonable person standard.[215] In other words, an allegedly objectionable publication must offend an "ordinary man."[216] This standard for private citizens in public places, rather than the standard for public figures that seek and enjoy publicity, arguably assists the protection of private citizens who desire to be left alone.[217] As noted previously, once an individual enters a public place, they do not expect to also enter cyberspace where vast online databases can be searched to discover personal information about the individual. In addition to the apparent benefits to private figures' privacy, the reasonable person standard has the practical advantage of limiting the amount of frivolous and extraneous information that can be reported about them; that is, things done or said by public figures are more likely to serve the public in an educational or newsworthy way than those said or done by private figures.[218] Much of the above discussion concerning the status of an individual entering public places centered on the

---

[212] *Time, Inc. v. Hill*, 385 U.S. 374, 388 (1967).
[213] James H. Barron, *Warren & Brandeis, The Right to Privacy 4 Harv. L. Rev. 193 (1890): Demystifying a Landmark Citation*, 13 Suffolk U. L. Rev. 875, 879-81 (1979).
[214] *Gill v. Hearst Pub. Co*., 40 Cal.2d 224.
[215] *Id*.
[216] *Id.*
[217] *Id.* (Carter, J. dissenting).
[218] *Id*.

press's right to publish newsworthy information. Therefore, in the context of networked wearable computers, the courts will have to determine the extent to which recordings of individuals in public places constitutes news; if the image constitutes news, then the newsworthy event will trump an individuals right to privacy in a public place.

FOURTH AMENDMENT LAW AND PRIVACY

The Fourth Amendment has been the main source of protection for an individual's privacy when a government actor is involved. The following section reviews Fourth Amendment search and seizure law in the context of privacy in public places. In the early twentieth century, the Supreme Court's Fourth Amendment jurisprudence was geared toward the protection of property.[219] The Court's inclination to protect property quite clearly is reflected in its 1928 decision in *Olmstead v. United States*.[220] In *Olmstead*, the Supreme Court held that use of a wiretap to intercept a private telephone conversation was not a "search" for purposes of the Fourth Amendment.[221] One of the grounds on which the Court justified its result was that there had been no physical intrusion into the person's home.[222] Under Olmstead's narrow view of the Fourth Amendment, the amendment was not applicable in the absence of physical intrusion, i.e., not applicable to public places.[223] Thus, without trespass or seizure of any material object, surveillance was beyond the scope of the Fourth Amendment as interpreted by the *Olmstead* Court.

However, in its well-known decision in *Katz v. United States*, decided 39 years after *Olmstead*, the Supreme Court rejected Olmstead's "trespass" doctrine, articulating, in its place, a Fourth Amendment jurisprudence based on the protection of individual

---

[219] *Olmstead v. United States*, 277 U.S. 438 (1928).
[220] *Id.*
[221] *Id*. at 454-455.
[222] *Id*. at 452.
[223] *Id.* at 452.

privacy.[224] In *Katz*, the Court held that the Fourth Amendment protected people, not places: "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[225] Thus, the Court held that physical penetration of a constitutionally protected area is not necessary before a search and seizure can be held to violate the Fourth Amendment. According to the Court in *Katz*, "once it is recognized that the Fourth Amendment protects people-and not simply "areas"- against unreasonable searches and seizures it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure."[226]

Changing technology precipitated the shift from protection of property to protection of privacy, and in 1968, just one year after *Katz,* Congress passed Title III of the Omnibus Crime Control and Safe Streets Act authorizing microphone surveillance or wiretapping for law enforcement purposes, and requiring a warrant based on probable cause, prior to such surveillance or wiretapping.[227] Specifically, Title III of the Omnibus Crime Control and Safe Streets Act as enacted regulated the interception of electronic, wire, and oral communication, but not video surveillance.[228] However, as federal courts have stated,[229] "video surveillance is more invasive of privacy than audio surveillance, 'just as a strip search is more invasive than a pat-down search'"; but Congress has not

---

[224] *Katz v. United States*, 389 U.S. 347 (1967).
[225] *Id.* at 351.
[226] *Id*. at 353.
[227] Omnibus Crime Control and Safe Streets Act of 1968, as amended, generally prohibits the interception of wire, electronic, and oral communications. *See* Title 18 U.S.C. § 2511(1)(a).
[228] 18 U.S.C. §§ 2510-2521 (1994). *See* Andrew Miller, *Electronic Surveillance*, 80 GEO. L.J. 1037 (1992).
[229] *U.S. v. Torres*, 751 F.2d 875 (7th Cir. 1984); *Messa-Rincon*, 911 F.2d 1433, 1442-1443 (10th Cir. 1990)..

made this distinction.[230] Therefore, there seems to be a deficiency in the law because video surveillance is unregulated by Title III, even though video is arguably more intrusive than aural (audio) surveillance.[231]

The use of video surveillance itself in the context of search and seizure law has been considered by different jurisdictions. The Sixth Circuit in *U.S. v. Torres*,[232] declined to hold that video surveillance was unconstitutional per se under the Federal Constitution's Fourth Amendment, and, more specifically, rejected the proposition that secretly videotaping in private places could never be considered reasonable under the Fourth Amendment. It was not meant to suggest, the court cautioned, that the Fourth Amendment was to be interpreted as allowing such surveillance to be used as generally as less intrusive techniques. A search could be unreasonable, though conducted under an otherwise valid warrant, the Court stated, if the search intruded on personal privacy to an extent disproportionate to the likely benefits from obtaining fuller compliance with the law.[233] Further, it was noted by the Ninth Circuit in *U.S. v. Taketa*,[234] that video surveillance did not, in itself, violate a reasonable expectation of privacy for purposes of the Federal Constitution's Fourth Amendment. And while expressing concern over the high degree of intrusiveness that was inherent in video surveillance, the court in *People v. Teicher,*[235] held that such surveillance was not per se unreasonable under the Federal Constitution's Fourth Amendment so as to require its prohibition in all circumstances.

---

[230] Thomas M. Messana, *Ricks v. State: Big Brother Has Arrived in Maryland*, 48 Md. L. Rev. 435, 452 (1989) (quoting Torres, *id*. at 885).

[231] People who are afraid of audio surveillance may mute or mask their conversations, move their conversations or communicate in non-verbal ways, but this is not possible with video surveillance.

[232] Torres, 751 F.2d 875.

[233] *Id.*

[234] *U.S. v. Taketa*, 923 F.2d 665 (9th Cir. 1991); *see also* U.S.C.A. Const. Amend. 4; *see also*, *U.S. v. Gonzalez*, 328 F.3d 543 (9th Cir. 2003)

[235] *People v. Teicher*, 422 N.E.2d 506 (1981).

Close scrutiny must be given to any application for a warrant permitting video surveillance, the court stated, but the Fourth Amendment did not mandate an absolute ban on such surveillance any more than it did with electronic eavesdropping.[236] It was also held in *State v. Clemmons*[237] that video surveillance as a method of investigation did not in itself violate a reasonable expectation of privacy under the Federal Constitution's Fourth Amendment, as the police could record what they could view with their naked eyes. Even though wearable computers can record and also analyze facial images, courts would likely hold that the analysis of a person's face using facial recognition software, if done in a public place, is not a search under the Fourth Amendment, as under *Clemmons*, all that would be recorded and analyzed is the same as what can be analyzed with the naked eyes. However, if the facial image was uploaded to the internet and paired with personal information, this change in facts may be sufficient for a court to find a violation of an individual's privacy.

A wearable computer system may contain sensors such as cameras, microphones, infrared and thermal heat sensors.[238] Would the information derived from the sensors constitute a search if performed by a government actor? In *Kyllo v. U.S*. the question considered by the Court was whether the use of a thermal-imaging device aimed at a private home from a public street to detect relative amounts of heat within the home constituted a "search" within the meaning of the Fourth Amendment.[239] The scan of Kyllo's home showed that the roof over the garage and a side wall of petitioner's home were relatively hot compared to the rest of the home and substantially warmer than

---

[236] *Id*.
[237] *State v. Clemmons*, 81 Wash. App. 1003, 1996 WL 146721 (Div. 1 1996).
[238] Jim Garamone, *Army Tests Land Warrior for 21st Century Soldiers*, *available at* http://www.defenselink.mil/news/Sep1998/n09111998_9809117.html (last visited Jan. 28, 2006).
[239] *Kyllo v. U.S*., 533 U.S. 27 (2001).

neighboring homes. The Court concluded that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical "intrusion into a constitutionally protected area," constituted a search-at least where (as here) the technology in question is not in general public use.[240] On the basis of this criterion, the Court concluded that the information obtained by the thermal imager in this case was the product of a search.[241] Therefore, when the ”Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a "search" and is presumptively unreasonable without a warrant.”[242] However, given the predicted increased usage of wearable computers, equipped with sense enhancing technology, they may become sufficiently mainstream technology so as not to constitute a search in Fourth Amendment terms; especially if used to record what is in plain sight or brought to the public.[243]

Although no court has ruled on the constitutionality of using wearable computers for purposes of surveillance by a government actor, the *Katz* doctrine leads to the nearly inevitable conclusion that the use of this technology - provided it occurs in a public place - is not a search.[244] In order to find that surveillance of individuals in a public place is a violation of the Fourth Amendment, the Supreme Court would have to reconsider one of the central aspects of the *Katz* doctrine - that a person is only protected if she enjoys a reasonable expectation of privacy in her actions. When this standard is applied to activity

---

[240] *Id*. at 31, 34.
[241] *Id.* at 40.
[242] *Id*. at 40.
[243] *See generally* Kang, *supra* note 2; Kang & Cuff*, supra* note 2.
[244] Under the FOIA, Exemption 7(C), the Government is allowed to refuse disclosure [of a picture] when somebody’s privacy interest in a requested document compiled for law enforcement purposes outweighs the public’s interest in disclosure.

in the public sphere, it is hard to conclude that the Fourth Amendment is implicated. Therefore, government actors using wearable computers may not be in violation of the Fourth Amendment when filming individuals in public places. In contrast, the courts have determined that the search if performed in a person's home and done by the media accompanying the police, does implicate the Fourth Amendment. For example, in "Reality TV" filming where the media accompanies law enforcement personnel in some variation of a "ride-along," if the media uses a video camera to record the police arrest and crime scene, the Fourth Amendment may be violated even if the individual is filmed in their own home.[245] On point is *Wilson v. Layne*,[246] where the Supreme Court held that media ride-alongs violated the Fourth Amendment when the media accompanied law enforcement officers into the person's home.[247]

VI. VIDEO VOYEURISM

This section of the article focuses on the use of wirelessly networked phone cameras in the context of video voyeurism, an emerging area of concern for invasion of individual's privacy in public places. Of interest to this article is that facial recognition software has been integrated into some phone cameras,[248] and that research is underway using Bluetooth-enabled camera cell phones that would record where the caller is, what time they called, and who they are with.[249] This later technology, which is being

---

[245] *See generally* David E. Bond*, Police Liability for the Media Ride-Along*, 77 B.U. L. Rev. 825 (1997).
[246] *Wilson v. Layne*, 526 U.S. 603 (1999).
[247] *Id*.; *see also* DeLeith Duke Gossett, *Constitutional Law and Criminal Procedure - Media Ride-Alongs into the Home: Can They Survive a Head-on Collision Between First and Fourth Amendment Rights*? *Wilson v. Layne*, 22 U. Ark. Little Rock L. Rev. 679 (2000); *but see infra* note 305 (the media entering a woman's home and taking her picture was not actionable).
[248] Dan Ilett, *Mobile Phones Get Facial Recognition*, *available at* http://www.cnet.com.au/mobilecomputing/pdas/0,39028789,40004440,00.htm (last visited Feb. 3, 2006).
[249] *Camera phone helps label snaps,* NewScientist.com news service *(2005) available at* http://www.newscientist.com/article.ns?id=mg18825314.300&feedId=online-news_rss20 (last visited Feb. 3, 2006).

developed at the University of California, Berkeley, in conjunction with Yahoo, is based on a central server that registers details sent by a cell phone when a photo is taken.[250] These include the nearest cell phone mast, the strength of the call signal and the time the photo was taken. The system also identifies other Bluetooth-enabled cell phones within range of the photographer and combines this with time and place information to create a shortlist of people who might be in the picture. This information can then be combined with facial-recognition software to identify the subjects from the shortlist, and to track the location of people. According to Professor Davis, a lead investigator on the project, facial recognition software on its own can only identify people with 43 per cent accuracy from the grainy shots taken by camera phones, but by combining facial recognition systems with context information the system may then correctly identify people 60 per cent of the time.[251] The context information can also be combined with image-recognition software to identify places within photos.[252] What this example illustrates is that wearable computer technology is converging such that it can not only record and analyze an individual's facial image but also track the individual in public places. The combination of these technologies may pose a significant threat to an individual's information privacy rights in public places. If we consider personal information to include where you are, who you are with, and what time you are there, especially if paired to other personal information about an individual that is searchable on the internet, this combination of

---

[250] *Id.*

[251] *Id.* In conjunction with Yahoo! Research Berkeley, *see* http://garage.sims.berkeley.edu/marc.cfm (last visited Feb. 8, 2006).

[252] *See generally* Marc Davis, Michael Smith, John Canny, Nathan Good, Simon King & Rajkumar Janakiraman. *Towards Context-Aware Face Recognition,* In: Proceedings of 13th Annual ACM International Conference on Multimedia (MM 2005) in Singapore, 483-486 (ACM Press 2005).

information may result in almost no privacy for any individual once they leave their house.

An important question that must be addressed in the area of privacy rights resulting from wearable computers equipped with facial recognition software, especially if personal information is paired to the facial image, is the appropriate cause of action to pursue by the aggrieved party. In some states, when a video camera is used to record an individual in an area where the person has a reasonable expectation of privacy, an action may be brought forth under a video voyeurism statute;[253] in other states there may be a right to privacy afforded in the state constitution.[254] For example, California, Alaska, and Hawaii[255] as well as other states, include a right to privacy in their respective state constitutions. And as noted in a previous section of this article, if the party doing the

---

[253] Matthew Keck, *Cookies, the Constitution, and the Common Law: A Framework for the Right of Privacy on the Internet*, 13 Alb. L.J. & Tech. 83, 91 (2002) ("…there have been many hearings in Congress and over 400 bills mentioning privacy have been proposed. In the state legislatures, the number of privacy-related bills that have been introduced is quadruple that.")

[254] Alaska Const. of 1956, art. I, 22 (1972) ("The right of the people to privacy is recognized and shall not be infringed. The legislature shall implement this section."); Ariz. Const. of 1912, art. II, 8 ("No person shall be disturbed in his private affairs, or his home invaded, without authority of law. "); Cal. Const. of 1879, 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."); Fla. Const. of 1969, art. I, 23 (1980) ("Every natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein."); Haw. Const. of 1959, art. I, 6 (1978) ("The right of the people to privacy is recognized and shall not be infringed without the showing of a compelling state interest."); Ill. Const. of 1971, art. I, 12 ("Every person shall find a certain remedy in the laws for all injuries and wrongs which he receives to his person, privacy, property or reputation. He shall obtain justice by law, freely, completely, and promptly."); La. Const. of 1974, art. I, 5 (1989) ("Every person shall be secure in his person, property, communications, houses, papers, and effects against unreasonable searches, seizures, or invasions of privacy."); Mont. Const. of 1973, art. II, 10 ("The right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest."); S.C. Const. of 1896, art. I, 10 ("The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures and unreasonable invasions of privacy shall not be violated. ..."); Wash. Const. of 1889, art. I, 7 ("No person shall be disturbed in his private affairs, or his home invaded, without authority of law.").

[255] *Id.*

filming is a government actor, the Fourth Amendment provides some, but limited, protection to individuals filmed in public places.[256]

Recent cases in video voyeurism dealing with the video taping and subsequent use of an individual's image without permission may provide some direction to the type of actions that may be pursued by a person filmed without permission by an individual with a wearable computer equipped with facial recognition software. Video voyeurism generally occurs when a person secretly films another person in an area where that person has a reasonable expectation of privacy, and has not consented to the observation.[257] Camera phones with wireless internet capabilities have been reported to be a voyeur's dream-come-true, pictures and even video can be shot "discreetly" and immediately emailed or uploaded to the internet.[258] Some victims of video voyeurism have sought relief through the claim of intentional infliction of emotional distress.[259] A court may hold a voyeur liable for causing severe emotional distress to a victim if the plaintiff can prove that the voyeur engaged in extreme or outrageous conduct and acted either intentionally or recklessly.[260] Although some claims have been successful under this tort action,[261] a plaintiff seeking relief from an unwanted picture may nevertheless find it

---

[256] *Supra,* Section V.

[257] *See generally* Ark.Code Ann. § 5-16-101, Crime of Video Voyeurism.

[258] *See generally Miller v. National Broadcasting Company*, 187 Cal. App. 3d 1463 (1986).

[259] *See* Clay Calvert & Justin Brown, *Video Voyeurism, Privacy, and the Internet: Exposing Peeping Toms in Cyberspac*e, 18 Cardozo Arts & Ent. L.J. 469, 558 (2002). *Anderson v. Fisher Broadcasting Cos*., 712 P.2d 803, 807 (Or. 1986) (recognizing a tort for invasion of privacy when the tortfeasor has the specific intent to cause plaintiff severe mental or emotional distress and such conduct exceeds "the farthest reach of socially tolerable behavior").

[260] *See* Restatement (Second) of Torts 46(1) (1965). "One who by extreme and outrageous conduct intentionally or recklessly causes severe emotional distress to another is subject to liability for such emotional distress, and if bodily harm to the other results from it, for such bodily harm." *Id*. A trier of fact will usually find outrageous conduct when the voyeur's actions have crossed all bounds of decency and are utterly intolerable in a civilized society. *Id*. at cmt. d.

[261] *See, e.g*., *Dana v. Oak Park Marina, Inc*., 660 N.Y.S.2d 906 (1997). Here, the owner of a marina installed surveillance cameras in the bathrooms of his establishment without providing any form of notice. *Id*. at 909-911. The court found that plaintiffs satisfied the prima facie elements of a claim for

difficult to convince a trier of fact that an indecent photo of herself in the hands of only one voyeur has caused severe emotional distress. However, with wirelessly networked technology such as a cell phone or video-based wearable computer, an image may be almost instantaneously posted on the internet, so far more than one individual may view the image, and indeed voyeurs often post the images to web sites frequented by other voyeurs.

In terms of additional causes of action, plaintiffs in video voyeurism cases have looked at Federal and state wiretapping statutes, but for the most part found them to be ineffective.[262] These statutes impose liability for unauthorized audio communications, but not the recording of a video image.[263] A few courts have, however, broadly interpreted "communication" within state statutes to include any exchange of thoughts, messages or information by a means other than spoken words.[264] On the other hand, federal courts have yet to include silent video recordings within the Electronic Communications Privacy

---

negligent and reckless infliction of emotional distress based on the fact that defendant videotaped them without their consent and later viewed the tapes with others at a personally owned bar for personal and unjustifiable purposes. *Id*. The court also refused to dismiss the claim based on statute of limitations. *Id*. at 911. The court reasoned that the statute of limitations began when the plaintiffs realized they had been video taped and not when the actual videotaping had occurred. *Id*.

[262] *See* 18 U.S.C. 2511 (2002). *But see* Deibler v. State, 776 A.2d 657 (2001). Defendant violated Maryland Wiretap Law, Md. Code Ann. 10-402(a)(1), when he placed a hidden camera "with audio accompaniment" in the victim's shower. *Id*. at 658. Maryland Wiretap Law makes it unlawful for any person to "willfully intercept...any wire, oral, or electronic communication." *Id*. at 660. In addition, the court found that the defendant was not required to know that his actions were unlawful in order to "willfully" violate the statute. *Id*. at 659.

[263] See 18 U.S.C. 2511(1) (2002): Any person who (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication; (b) intentionally uses, endeavors to use, or procures any other person to use any electronic, mechanical, or other device to intercept any oral communication...shall be punished. *Id*. *See also* 18 U.S.C. 2510(5). The Code defines "electronic, mechanical or other devise" as "any device or apparatus which can be used to intercept a wire, oral or electronic communication ... ." *Id*.

[264] See *People v. Gibbons*, 215 Cal.App.3d 1204 (1989). The defendant invited three women into his home and videotaped their sexual encounters without the consent of any of the women. *Id*. Under California Penal Code section 632 , it is a crime to record a confidential "communication." *Id*. The court rejected defendant's argument that the statute did not extend to recording of sexual acts and held that the statute did apply to the surreptitious recording of this type of expressive conduct. *Id.* Rather than reading the statute narrowly, the court reached its decision by relying on the legislative intent of the statute, which was to protect the privacy rights of Californians. *Id.*

Act.[265] Therefore, video voyeurs can escape liability under wiretapping statutes by either photographing the victims or videotaping them without using sound.[266]

To address the problem of cell phone video voyeurism, a recent bill signed into federal law[267] was enacted to ban the use of camera-equipped phones when used to photograph or videotape a disrobed person without his or her consent in any place where there can be "a reasonable expectation of privacy." The key language of the Federal statute is:

> "Whoever, in the special maritime and territorial jurisdiction of the United States, has the intent to capture an image of a private area of an individual without their consent, and knowingly does so under circumstances in which the individual has a reasonable expectation of privacy, shall be fined under this title or imprisoned not more than one year, or both." Title 18 § 1801.

Some terminology and definitions in the Federal Video Voyeurism statute have relevance for a statute which would address information privacy violations involving a

---

[265] See 18 U.S.C.S. 2511(1) (2002). *See also United States v. Koyomejian*, 970 F.2d 536 (9th Cir. 1992), cert. denied, *Koyomejian v. United States*, 506 U.S. 1005 (1992). Plaintiffs were suspected of money laundering and drug trafficking. *Id*. at 538. Although the district court gave the government permission to install microphones and hidden television cameras in plaintiffs' office, the court granted plaintiffs' motion to suppress evidence. *Id*. The district court held that domestic silent video surveillance was prohibited by Title I of the Electronic Communications Privacy Act. *Id*. On appeal, the court found that domestic silent video surveillance was neither regulated nor prohibited by 18 U.S.C.S. 2510. *Id*. The appellate court cited to the legislative history of Title I, which revealed that the United States Senate did not intend to include other forms of surveillance outside of oral communication. *Id*. at 539. The appellate court also held, however, that silent video surveillance is subject to the Fourth Amendment and remanded the case for further analysis. *Koyomejian*, *id*. at 541. The appellate court cited Rule 41(b) of the Federal Rules of Criminal Procedure, which authorizes a district court to issue warrants for silent video surveillance, and stated that the district courts must ensure that the basic requirements of issuing warrants are followed in accordance with Title I. *Id*. at 542. One such requirement was that the warrant must require that the surveillance be conducted in such a way as to minimize the videotaping of activity not otherwise subject to surveillance. *Id.* In spite of this holding, the Fourth Amendment has yet to be expanded to include acts of video voyeurism. *See, e.*g., *See State of Washington v. Glas*, 147 Wash.2d 410, 54 P.3d 147, (2002).

[266] *See* Clay Calvert & Justin Brown, *Video Voyeurism, Privacy, and the Internet: Exposing Peeping Toms in Cyberspac*e, 18 Cardozo Arts & Ent. L.J. 469 (2002).

[267] Title 18 § 1801, Video Voyeurism Prevention Act of 2004, the law is targeted at camera-equipped cellphones and is designed to prohibit photographing or videotaping a naked person without his or her consent in any place where there can be "a reasonable expectation of privacy." *Id. Also see Federal Video Voyeurism Prevention Act Aims to Protect Privacy in Public Places,* Mark S. Sullivan, Medill News Service (2004). The article explains Just under 9 million of the camera phones were shipped to the U.S. during 2003, that number is expected to surpass 27 million in 2004, and may reach 100 million in 2008, *available at* http://www.pcworld.com/news/article/0,aid,117035,00.asp (last visited Feb. 2, 2006).

wirelessly networked video-based wearable computer. For example, as described in the statute, to `capture' an image means to videotape, photograph, film, record by any means, or broadcast; whereas; `broadcast' means to electronically transmit a visual image with the intent such that it be viewed by a person or persons.[268] However, a key term under the Federal Video Voyeurism Statute- `under circumstances in which that individual has a reasonable expectation of privacy' would need to be modified to accommodate information privacy in public places. Regarding an information privacy statute, a 'reasonable expectation of information privacy' would need to be designed to protect a persons privacy who had entered a public place, was filmed by a wearable computer, and had their image posted on the internet along with personal information.

A growing number of states have also enacting legislation to address the problem of video voyeurism.[269] For example, New York State enacted legislation termed "Stephanie's Law" that creates criminal penalties for acts of video voyeurism.[270] Specifically, Stephanie's Law creates criminal penalties for those who would use a mechanical, digital or electronic device to capture visual images of another person in a place where that person had a reasonable expectation of privacy and had not given his or her consent.[271] Stephanie's law also creates criminal penalties for those who disseminate, publish, or sell images of the intimate parts of another person's body. The legislation requires that a video voyeur who is caught using or installing a camera for sexual purposes, or in a bedroom, bathroom, or other specified rooms, would be subject to

---

[268] Title 18 § 1801.
[269] Kathryn Williams**,** *Policing Video Voyeurs*, *The Feds Join the Battle Against Perverts with Cameras*, "Currently 44 states h ave some kind of statute that make video voyeurism a crime," Newsweek, 2006, *available at* http://www.msnbc.msn.com/id/6919996/site/newsweek/#storyContinued (last visited Jan. 29, 2006).
[270] New York, 60 § 1, Stephanie's Law.
[271] *Id*.

presumptive registration with the State's Sex Offender Registry. Under Stephanie's law, a person with a wearable computer filming the intimate parts of another, would be liable just as would any other voyeur using video equipment.

In New York, there is also a General Business Law statute that forbids an "owner or manager" of a premise to knowingly permit or allow a viewing device to be installed or maintained in such premise for the purpose of surreptitiously observing, or recording a visual image in, the interior of "any fitting room, restroom, toilet, bathroom, washroom, shower, or any room assigned to guests or patrons in a motel, hotel or inn."[272] Under such a law, would the proprietor of the premise be required to ask an individual equipped with a video-based wearable computer to leave the premise? The proscribed act is a violation if the conduct is limited to "observing"; it is a felony if the conduct is "recording."[273] The General Business Law applies only to the "owner or manager" of the premise, and the General Business Law prohibition does not apply to a "private dwelling" or to certain other locations which are covered by the Penal Law crimes.[274]

In video voyeurism, the place and time when a person has a reasonable expectation of privacy, is an important aspect of video voyeurism statutes and may turn out to be the one most litigated. The notion of a reasonable expectation of privacy is also central to the intrusion into a person's privacy in a public place if one is considering the concept of information privacy. The "reasonable person" definition in video voyeurism statutes borrows the terminology from Fourth Amendment's "reasonable expectation of privacy" case law.[275] A "reasonable expectation of privacy" reflects whether the person

---

[272] New York, General Business Law § 395-b.
[273] *Id*.
[274] *Id*.
[275] *See, e.g*., Katz*, supra* note 224; *Smith v. Maryland*, 442 U.S. 735, 743-744 (1979).

viewed has a subjective expectation of privacy at the time and place of the viewing, and if so, whether from an objective standpoint it is an expectation that accords with societal conventions. This article argues that personal information disseminated on the internet and paired to a person's image would diverge from societal expectations of what privacy a reasonable person should expect when they enter a public place; and thus should be actionable.

Permitting one's self to be filmed with knowledge that you are being viewed is a form of implied consent. Therefore, there would be no "expectation of privacy" under an information privacy statute in knowingly exposing oneself to a person with a video-based wearable computer. Here the concept of physically exposing yourself to being filmed versus exposing an individual's personal information when they enter a public place differs. While an individual may knowingly expose their image to the public once they enter a public place, they do not knowingly or purposively expose personal information about themselves when they enter a public place; the personal records of their affairs are expected to be kept private and "at home." Based on Prosser's analysis of tort law, the image recorded by the video-based wearable computer in a public place may be considered public information. However, personal and private facts associated with the image, especially if posted on the internet would be considered personal, and nonpublic information. Essentially, with video-based wearable computer technology, once a person enters a public place, they may also unknowingly be entering cyberspace as their image may be recorded, analyzed, and uploaded to the internet. The law as currently developed, offers some privacy protection for cyberspace transactions on the internet, but does not

consider the combination of public and cyberspace privacy in the age of wirelessly wearable computers.

The video voyeurism statutes enacted in some states have already resulted in prosecution, and such prosecution may be illustrative for disputes that may involve wearable computers and privacy. The road toward the Federal video voyeurism law began with two state cases, one in Louisiana and one in Washington State; in both, video technology was used to violate an individual's privacy. In the first case, Susan and Gary Wilson of Monroe, Louisiana discovered that a neighbor had installed hidden cameras in the Wilson's master bedroom and bathroom.[276] To the Wilson's surprise, Louisiana authorities said their neighbor's actions were not criminal offenses under current state and federal law. After the Wilson's learned their neighbor had similarly victimized others in the community, the couple urged their state representatives to change the law. In 1999, the Louisiana governor signed a bill making video voyeurism a felony.[277]

The second case which influenced Federal law makers occurred in Washington State, where Richard Sorrells secretly aimed a video camera up a woman's skirt as she waited at an ice cream stand during a festival in 2000.[278] The Washington State Supreme Court ruled that filming up women's skirts, though "disgusting and reprehensible," wasn't in violation of current state law.[279] It overturned the convictions of Sorrells and another man, Glas, who was accused of taking photographs under women's skirts at a shopping mall. In response to the outcome of these cases, in 2002, Washington state lawmakers changed the law to give legal recourse to people whose privacy was violated in public.

---

[276] Stephanie L. Brooke, *Is Cyber Peeping Causing Future Shock*? 4 Expository Magazine, *available at* http://www.expositorymagazine.net/2004/september/cyberpeeping.php (last visited Jan. 28, 2006).
[277] Louisiana, La. R. S. §14:284 (2002).
[278] *See State of Washington v. Glas*, 147 Wash.2d 410.
[279] *Id*.

The new law was used to prosecute Jack Le Vu, the first known cell phone camera voyeur to be convicted in the United States.[280] In 2003, Vu was seen in a Seattle area Safeway using a cell phone camera to covertly snap pictures beneath the skirt of a woman shopping next to him. Under the revamped Washington privacy law, Vu was successfully prosecuted and later pleaded guilty to one count of voyeurism.[281] He was sentenced to 60 days jail time and forced to register as a sex offender.[282]

VII. REALITY FILMING, STILL PHOTOGRAPHS AND PRIVACY

"Reality filming" and the use of photographs of individuals taken in public places are both areas where there have been disputes involving alleged invasions of privacy. Some aspects of the cases in these areas have "voyeuristic" components, and thus relate to the previous material in this article; however, each area brings up some new issues not covered in the previous section. Americans have long been fascinated with the personal affairs of other people, *Warren and Brandeis* spoke of this in their 1980's article.[283] More recently, in the 1990's an abundance of "reality" television shows which focused on the private lives of individuals appeared, including: COPS, I-Witness Video, Firefighters, Real Stories of the Highway Patrol, Emergency Response, and Rescue 911.[284] For example, in the United States, camera crews often follow police and emergency personnel as well as use video surveillance cameras mounted on poles and buildings in

---

[280] Mark S. Sullivan Medill, *Law May Curb Cell Phone Camera Use*, *Federal Video Voyeurism Prevention Act Aims to Protect Privacy in Public Places*, *available at* http://www.pcworld.com/news/article/0,aid,117035,00.asp (last visited Jan. 28, 2006).

[281] Jesse J. Holland, *Cell Phone Camera Crackdown*, *available at* http://www.cbsnews.com/stories/2004/05/11/tech/main616694.shtml (last visited Feb. 2, 2006).

[282] *Id*.

[283] Warren & Brandeis, *supra* note 19.

[284] McClurg, *supra* note 15, at 1013. McClurg believes that the aspiration of these programs is to compact as much human suffering and embarrassment as possible into a 30 or 60 minute telecast. *Id*.

order to film individuals without their permission.[285] Such programs highlight the extremely personal information that reality television may reveal about an individual, just as can video-based wearable computers.[286] For example, in the mid 1990's Langley Productions marketed a "too hot" for television version of COPS that the "censors would not let you see."[287] The most graphic portions of the video showed a man who hung himself in his garage, a drive-by shooting victim dying in a car, a man running from his house on fire and the deceased bodies of an entire family including a baby in a crib.[288] Another "reality" show placed a hidden microphone on a paramedic who aided a critically injured woman who could be heard begging for her life.[289] Moreover, news tabloid shows and other news programs constantly use hidden cameras and microphones to expose the personal details of an individuals life.[290] One commentator concluded that

---

[285] Another growing trend is the mounting of cameras on police cars and in police cars. C. Ron Allen, *Boca Police Put Motorists on Candid Camera*, SUN- SENTINEL (Ft. Lauderdale), May 15, 1995, at 3B. In Florida, these mounted cameras are used in conjunction with microphones worn by the police officers when they pull over a car. *Id.* The cameras are typically used to help document drunk driving arrests. *Id.* Although the police do not need to let the people know that they are being filmed, the officers inform the motorists that they are being filmed and audiotaped. *Id.* This seems slightly different than street surveillance cameras because the person already knows the officer is observing them, and they are also informed that a video and audio tape is being made. The police in California have also installed cameras in patrol cars as a result of the Rodney King beating in 1991. Patrick McGreevy, *Chief Wants Squad-Car Cameras Kept on During Specific Operations*, L.A. DAILY NEWS, July 15, 1995, at N3. The video cameras are to be turned on during pursuits, traffic stops, and traffic-related investigations for evidence purposes and to help reduce conflicts between officers and citizens. *Id*. *See also Haymond v. Dep't of Licensing*, 872 P.2d 61, 63 (Wash. Ct. App. 1994) (upholding the use of a video camera during a traffic stop without the driver's consent).

[286] The internet is also used to market reality filming subject matter as well.

[287] *COPS: Too Hot For TV, Volume I*, (Barbour/Langley Productions 1995). This video includes footage of drunk drivers humiliating themselves, women and men engaged in prostitution, women offering police sexual favors, and full frontal nudity of men and women. The video also includes at least five requests by different individuals to "get the camera out of here," which the camera-operators totally ignore. Moreover, many people are shown without the face distortion technique often used on the television show. *Id.*

[288] *Id*.

[289] Gail Diane Cox, *Privacy Frontiers At Issue: Unwilling Subjects of Tabloid TV Are Suing*, 16 NAT'L L.J. 1 (1993).

[290] McClurg, *supra* note 15, at 1014. Don Hewitt, the executive producer of 60 Minutes, recently stated that: "It's a small crime versus the greater good. . .. If you can catch someone violating 'thou shall not steal' by violating 'thou shall not lie,' that's a pretty good trade-off." *Id*. at 1015 n.129 (citing Howard

it seems that the voyeurism market has advanced to the point where cameras are so widespread, that people in public places are left with little, if any, privacy.[291]

However, even given the extreme graphic content of the above examples, the law may under limited circumstances provide protection for a person's privacy when they have been filmed in a public place. For example, in one case a plaintiff was able to recover for a photograph taken of her in public when an air jet blew her skirt over her head.[292] The photographer sold the picture of the woman in her underwear to a newspaper which published the photograph on the front page of its paper.[293] An important distinction made by the court was that the intrusion into privacy occurred the moment the photograph was taken, not when the photograph was published.[294] The use of wearable computers by individuals in public places may easily result in similar recordings of an individual in a compromising position, and thus based on the above decision, may violate the person's privacy at the moment of filming. In another case limiting the right to film an individual in a public place, the California Supreme Court in 1998 ruled against the producers of *On Scene: Emergency Response* for videotaping conversations between a car-accident victim and a nurse on a medical evacuation

---

Kurtz, Hidden Network Cameras: A Troubling Trend? Critics Complain of Deception as Dramatic Footage Yields High Ratings, WASH. POST, Nov. 30, 1992, at A1).

[291] McClurg, *supra* note 15, at 1080. *See also* Mark Levy, *Of Laws and Lenses*, Videomaker (Magazine), Dec. 1995, at 76. A person does not have the absolute right to include even true statements about another in a video without permission. *Id*. at 78. Videotaping a person's private conversations or his family and business activities without permission constitutes an invasion of privacy. *Id*. Public interest should not be the standard by which the courts judge the acceptability of privacy intrusions. McClurg, *supra* note 15, at 1080.

[292] *Daily Times Democrat v. Graham*, 162 So.2d 474 (Ala. 1964).

[293] *Id*. at 476. The court called the photograph a "wrongful intrusion into one's private activities." *Id*.

[294] McClurg, *supra* note 15, at 1073. However, McClurg argues that to discount the publication aspect of the privacy tort would be like focusing on the pin prick in a person's arm when they are infected with HIV through a blood transfusion instead of focusing on the offensiveness and intrusiveness of infecting the person. *Id*. at 1075.

helicopter.[295] The U.S. Supreme Court also ruled in 1999 that police may have violated the privacy rights of citizens by allowing *Washington Post* reporters to tag along when they questioned the parents of a criminal suspect in their home.[296] While the crash scene itself was newsworthy and exempt from suit, the court ruled, the victim had a reasonable expectation of privacy in the helicopter.[297]

But in most cases when a person has been filmed in a public place, the plaintiff's privacy claim fails especially, if as noted previously, the defendant is able to successfully use a "newsworthy" defense. For example, a couple tried to sue the publisher of "World Guide to Nude Beaches and Recreation" after he published a photograph of them on a nude beach.[298] The Appellate Court in New York held that the matter was of some public interest, and the couple's picture was reasonably related to the subject; therefore, the couple was not allowed to recover.[299] In another case, *Jones v. Herald Post Co*.,[300] the plaintiff brought an action for the invasion of her privacy as a result of the publication of a picture that related to the death or her husband. The court, in denying the right of the plaintiff to recover, stated in part as follows: "The right of privacy may be defined as the right to live one's life in seclusion, without being subjected to unwarranted and undesired publicity. In short, it is the right to be let alone."[301] There are times, however, when one, whether willingly or not, becomes an actor in an occurrence of public or general interest, when this takes place, he emerges from his seclusion, and it is not an invasion of his right

---

[295] *Shulman v. Group W Productions, Inc*., 955 P.2d 469 (Cal.Sup.Ct. 1998).
[296] *Wilson v. Layne*, 526 U.S. at 607-608, 613.
[297] Congress complicated things in 2001 with the Health Insurance Portability and Accountability Act, or HIPAA, which requires health care providers to prevent the unauthorized disclosure of medical information. This Act has severely impacted the business of medical-themed reality shows.
[298] *Creel v. Crown Publishers*, 496 N.Y.S.2d 219 (N.Y. App. Div. 1985). The book contained 200 close-up photographs of nudes. *Id.* at 220.
[299] *Id*.
[300] *Jones v. Herald Post Co*., 230 Ky. 227 (18 S. W. 2d 972),
[301] 21 R. C. L. 1197, 1198

of privacy to publish his photograph with an account of such occurrence.[302] In a similar case, a Georgia newspaper published photographs of a murdered fourteen-year-old girl whose body was partially decomposed and wrapped in chains.[303] A Georgia court held that the girls body was newsworthy and the girl's family could not maintain a cause of action.[304] In a particularly egregious case which involved the newsworthiness of the story versus the privacy rights of the plaintiff, a woman's former husband kidnapped her, took her to an apartment, and stripped and raped her.[305] The police arrived with camera crews, and although the woman attempted to cover herself with a dish towel, her photograph was published the next day in a newspaper.[306] A Florida court seeming to conclude that voyeurism was a protected right, denied the woman damages, and held that the event was a newsworthy, emotion-packed drama to which others are attracted.[307] Based on the above court decisions, the courts take a liberal view as to what captures the publics interest; and if the court finds that the recorded incident is a matter of public interest, or matter of a public investigation, a publication in connection therewith will in most jurisdictions not constitute a violation of one's legal right of privacy.

A few additional issues of relevance for video-based wearable computers is whether the recorded image is used for a commercial or noncommercial use, and whether the recorded image is used for a political or nonpolitical use. In a dispute involving the use of a photograph without permission, a multi-million dollar lawsuit was filed against a

---

[302] *Id.*
[303] *Waters v. Fleetwood*, 91 S.E.2d 344 (Ga. 1956).
[304] *Id.*
[305] *Cape Publications, Inc. v. Bridges*, 423 So.2d 426 (Fla. 1982). Hilda Bridges was abducted by her estranged husband who came to her workplace and forced her at gunpoint to go with him to their former apartment. *Id*. at 427.
[306] *Id*. The police heard a gunshot, stormed the apartment and rushed Bridges outside to safety. *Id*.
[307] *Id*. "At some point the public's interest in obtaining information becomes dominant over the individual's right of privacy." *Id*. at 427. A hypersensitive individual will not be protected under an invasion of privacy. *Id*.

political activists group and a political consulting firm for allegedly stealing a gay couple's wedding photo and using it in a political ad.[308] The suit alleged numerous complaints- that the use of the couple's image without permission constituted an invasion of privacy, was libelous, placed them in a false light, violated their right of publicity, and constituted an intentional infliction of emotional distress.[309] This particular case illustrates how the facts surrounding the case influence the direction of the litigation. To wit, when pictures and video are used in political ads, they are treated as fully protected speech under the First Amendment, and not as the less protected "commercial speech."[310] Moreover, when the claim involves speech on matters of public concern, courts generally reject the claim on First Amendment grounds.[311] This discussion suggests that to the extent an image recorded by a wearable computer is used for a purpose protected by the First Amendment, such as political speech, it may not violate a person's privacy.

The case of *Lane v. MRA Holdings, LLC*,[312] presented earlier in this article is representative of a recent trend in reality filming. The dispute involved the use of an image in a "Girls Gone Wild" commercials and video. The plaintiff argued that the use of the video in the film was not expected because she was told while being filmed by the cameraman that he was intending to make a film for his own personal use. According to the plaintiff, Lane, the cameraman represented to her that he would not show the video to

---

[308] *The Volokh Conspiracy*, *available at* http://volokh.com/posts/chain_1110553327.shtml (last visited Jan. 28, 2006).
[309] *Id*.
[310] *Central Hudson Gas & Electric Co. v. Public Service Commission*, 447 U.S. 557 (1980) (discussing the four-point test used for evaluating the constitutionality of government regulations on commercial speech).
[311] *Id*. According to Professor Volokh the strongest claim against USA Next would be a copyright claim brought by the copyright owner, which seems to be the Portland Tribune newspaper (or perhaps the photographer, if he was a freelancer and kept the copyright).
[312] Lane v. MRA Holdings, 242 F.Supp.2d 1205.

anyone who was not present at that time.[313] The first three counts of Lane's claims were brought under Florida law against MRA for unauthorized publication in violation of common law invasion of privacy for commercial misappropriation of likeness and false light invasion of privacy.[314] Under Florida law, the elements of common law invasion of privacy for commercial misappropriation of likeness, coincide with the elements of unauthorized publication of a name or likeness in violation of Fla. Stat. § 540.08.[315] MRA argued that Fla. Stat. § 540.08 absorbed the common law claim of invasion of privacy based upon a commercial misappropriation of likeness. However, section 6 of Fla. Stat. § 540.08 provides that the "remedies provided for in this section shall be in addition to, and not in limitation of the remedies and rights of any person under the common law against the invasion of her or his privacy."[316]

Lane also asserted a claim against MRA for false light invasion of privacy. According to Lane, MRA's juxtaposition of her with other women exposing their genital areas, or engaging in extended topless and suggestive dancing portrayed her in a false light. The two essential elements for recovery under false light invasion of privacy are: (1) the false light must be highly offensive to a reasonable person; and (2) the defendant must have acted either knowingly or in reckless disregard as to the falsity of the publicized material and the false light in which it would be placed.[317] With regards to the first element the court concluded that although a reasonable jury could conclude that the

---

[313] *Id*.
[314] *Id.*
[315] *See Heath v. Playboy Enters., Inc.,* 732 F.Supp. 1145, 1147-1148 (S.D.Fla.1990) (noting that fourth theory of recovery under common law invasion of privacy, "appropriation for commercial benefit, is statutory in Florida"); *Loft v. Fuller,* 408 So.2d 619, 622 (Fla. 4th DCA 1981) ("By enacting section 540.08, the Florida Legislature has amplified the remedies available for the fourth form of invasion of privacy: commercial exploitation of the property value of a person's name or personality").
[316] FLA. STAT. § 540.08.
[317] See *Harris v. Dist. Bd. of Trs. of Polk Cmty. College*, 9 F.Supp.2d 1319, 1329 (M.D.Fla.1998); *see also* Section 652(e) of the Restatement (Second) of Torts.

use of Lane's image and likeness in a video containing women exposing themselves is highly offensive, no reasonable jury could conclude that Girls Gone Wild or its marketing campaign with *Sexy Sorority Sweethearts* placed Lane in a false light.[318] Foremost, the court reasoned that in the video, Lane is depicted truthfully and accurately as doing exactly what she did, exposing her breasts on a street in Panama City in exchange for a beaded necklace.[319] Moreover, the court concluded, considering the nature of Lane's actions, the publication of her image in a video containing other women engaging in similar acts was neither unreasonable nor inaccurate.[320] Altogether, MRA's juxtaposition of Lane with other women exposing themselves cannot give rise to the tort of false light invasion of privacy because the depiction of Lane was reasonable, accurate, and truthful.[321] The court reasoned that if the publicity is an accurate portrayal of the public display, if the publicity is not unreasonable and false, then Lane has no actionable privacy interest, even if the publicity has caused embarrassment, offense, or damage.[322]

VI. TOWARDS AN INFORMATION PRIVACY STATUTE

As shown above, current law dealing with video recordings in public places is represented by a patchwork of statutes and common law causes of action, with no specific law covering the capability of wearable computers to invade an individual's

---

[318] *Id*.
[319] Lane v. MRA Holdings, 242 F.Supp.2d 1205.
[320] *Id.*
[321] *Easter Seal Soc. for Crippled Children & Adults v. Playboy Enters., Inc*., 530 So.2d 643, 647 (La.App.1988) ("[t]he tort of false light invasion of privacy affronts that private self by publishing a public display in a manner which is both unreasonable and false").
[322] *Id*. (holding that the use of a clip from a Mardi Gras parade in a Playboy movie focusing on sex and drugs could not support a false light claim because although the publicity could have caused embarrassment, offense, or damage, "if the publicity is not unreasonable and false, then plaintiff has no actionable privacy interest").

privacy in a public place.[323] While in the past, a person who entered a public place was said to place themselves under the general scrutiny of the public's eyes, the public's ability to know personal information about an individual was limited to what their naked eyes could discern. However, networked wearable computers with facial recognition software has changed this basic premise; if an individual's image can be identified and uploaded to the internet, a tremendous amount of personal information can be known and paired to a particular individual. Now days, a person entering public space, may unknowingly be entering cyberspace; yet the law on privacy has not adapted to this reality. In this regard, Professor Froomkin observed that as a result of modern surveillance technology, there was an erosion of the border separating the private from the public spheres.[324] This article argues that in an age of wirelessly networked and video-based wearable computers, legislatures should enact a statute which would protect the information privacy rights of individuals in public places.[325]

The right to information privacy as advocated in this article and by legal scholars,[326] is not a new concept, in fact it was addressed by the U. S. Supreme Court in

---

[323] *See generally*, Joel R. Reidenberg, *Restoring America's Privacy in Electronic Commerce*, 14 Berkeley Tech. L. J. 771 (1999). 138 Cong. Rec. E81-02 (extension of remarks Jan. 24, 1992) (statement of Rep. Lee H. Hamilton). "The Congress and the President must devise a better framework for safeguarding privacy rights in an era of rapid technological innovation." Id. at E82. Covert video surveillance is not covered by federal wiretapping statutes and bills that have been introduced to amend Title III have been rejected. 136 Cong. Rec. E2297-01, E2298 (July 11, 1990) (statement of Rep. Don Edwards). Although Representative Kastenmier introduced a bill in 1984 to extend Title III protection to video surveillance, it did not pass by the end of the 98th Congress, and it has never been resubmitted. H.R. 6343, 98th Cong. (1984). Representative Kastenmier declared that this bill would apply to both private and public sources in closing the video loopholes of Title III. 130 Cong. Rec. E4107-08 (daily ed. Oct. 1, 1984) (statement of Rep. Kastenmier). *See also* Nancy J. Montroy, *United States v. Torres: The Need for Statutory Regulation of Video Surveillance*, 12 Notre Dame J. Legis. 264, 264-274 (1985).

[324] Froomkin, *supra* note 51.

[325] Nancy J. Montroy, *United States v. Torres: The Need for Statutory Regulation of Video Surveillance*, 12 Notre Dame J. Legis. 264, 264-274 (1985).

[326] *See e.g.*, Kang *supra* note 2.

Whalen v. Roe almost 30 years ago.[327] The *Whalen* case involved the invasion of patients' privacy by a New York statute requiring physicians to submit copies of prescriptions for abused drugs to the state for inclusion in a centralized computer file.[328] While the Court upheld the statute, finding that New York's interest in experimenting with solutions to control the distribution of dangerous drugs was a legitimate exercise of the state's police power; still the Court affirmed the right of an individual to have his personal information kept private.[329] The court stated:

> A final word about issues we have not decided. We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of the criminal laws all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed. The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures.[330]

Later, in 1989, the Supreme Court described the right to privacy as encompassing "the individual's control of information concerning his or her person."[331] More recently, Professor Kang adopted the Supreme Courts description of information privacy in his call for an "Information Privacy Act," describing information privacy as an individual's personal information and his ability to control that information.[332] As an extension to this concept, it has been argued that information privacy should include more than just control over personal information, but should also include information that expresses one's

---

[327] *Whalen v. Roe,* 429 U.S. 589 (1977).
[328] *Id*. at 589-591.
[329] *Id*. at 596-605.
[330] *Id*. at 605. *See also Id*. at 598-600, nn.22-26 (noting that courts have recognized a privacy interest in avoiding disclosure of personal matters).
[331] *United States Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 763 (1989).
[332] *See* Kang, *supra* note 2.

identity; for example, information that can be used to place individuals into categories.[333] Karas noted that under such an approach, when determining whether a privacy violation had occurred, "a court would consider whether one's privacy as a consumer, a sexual being, a father, etc. had been invaded by a particular practice."[334] This idea seems to be compatible with the Fourth Amendment's case law discussing the "standard of a reasonable person" to determine if an individual should have an expectation of privacy in a public place.[335] However, under Karas's view, the standard of a reasonable person within a particular category would have to be determined, as would the number and type of categories; such an approach may be unworkable unless the categories were limited and the procedure for identifying individuals within a category were clear and easily determined.

As discussed in this article, given the capabilities of wirelessly networked video-based wearable computers with facial recognition software, and tracking technologies, much personal information about an individual can be known and paired to an individual's image. On this point, one need not be concerned with just the capability of wearable computers to track individuals and invade their privacy, as Professor Schwartz has outlined, implantable chip technology can also be used to track a person and collect extensive and continuous personal data about them.[336] Given the ability to track an individual, a particular type of wearable computer, those with opaque or see-through displays, may result in an even greater invasion of a person's privacy than filming an individual and uploading their image to the internet. Wearable computers with opaque or

---

[333] Stan Karas, *Privacy, Identity, Databases*, 52 Am. U.L. Rev. 393, 427 (2002).
[334] *Id* at 428.
[335] *See* Prosser, *supra* note 130; *See, e.g.*, Katz*, supra* note 224; *Smith v. Maryland*, 442 U.S. 735, 743-744 (1979)
[336] Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 Harv. L. Rev. 2055 (2004).

see-through displays may allow personal information to be directly "pasted" on an individual's image as they move around public places.[337] What is troublesome about such technology is that the ability to track a person's movements and to pair personal information to an individual based on where they are at a given time, may provide useful information to stalkers, pedophiles, and other criminals. Stalkers have been known to use video cameras to monitor their victims movements, which is often a precursor to a violent crime.[338] On this point, some states have included language in their stalking statute which specifically mentions surveillance as an act of stalking.[339] Further, pedophiles often like to know the location and identity of kids as kids move around public places in order to alert other pedophiles. The law on tracking individuals is unsettled, while an individual may not stalk a person, a Federal circuit has held that it is not a search under the Fourth Amendment for the police to place a GPS unit on a suspect's car; in contrast, a New York State court ruled that such an act is a search.[340]

In an age of wearable computers, based on privacy and safety concerns, there needs to be a comprehensive federal policy guaranteeing an individual the right to control the collection and distribution of their personal information once they enter a public place. Such a statue should include the ability to control the dissemination of location data and whether an individual's image may be filmed, analyzed, and uploaded to the

---

[337] *See generally* Mann, *supra* note 25.

[338] *H.E.S. v. J.E.S.*, 793 A.2d 780 (N.J.Ct.App 2002). As reported by the Kansas Coalition Against Sexual and Domestic Violence, over 500,000 woman, and over 180,000 men are stalked each year by an intimate partner (citing P. Tjaden & N. Thoennes, Extent, Nature, and Consequences of Intimate Partner Violence (NMCJ 181867)), Washington DC: U.S. Department of Justice, National Institute of Justice and Centers for Disease Control and Prevention, *available at* http://www.kcsdv.org/state.html (last visited Feb. 11, 2006).

[339] *See* Arizona, A.R.S. § 13_2921 (2001); Colorado, C.R.S. § 18-8-111 (2001); Georgia, O.C.G.A. § 16-5-90 (2001); Hawaii, HRS § 711-1106.5 (2001); and South Carolina, S.C. Code Ann. § 16-3-1700 (2001).

[340] *Federal Judge's Ruling on the Use of GPS Worries Privacy Advocates*, *available at* http://www.infowars.com/articles/bb/ruling_on_gps_worries_privacy_advocates.htm (last visited Fed. 11, 2006).

internet. While these last categories of information- location data, and the video recording and identification of an individual's image, are normally not considered under the rubric of personal information- we have now entered a technological age where the identity of a person and their location are considered highly sought after information by marketers[341] and others who may use such information for nefarious reasons- thus the law ought to consider whether such information should be regulated.

If a statute were to be enacted to protect an individuals information privacy rights in a public place, what would be the basic components of such a statute? In the context of information privacy, Kang discussed personal information as "information identifiable to the individual."[342] He also indicated that "personal" in the context of information did not necessarily mean sensitive, private, or embarrassing information, but that it described a relationship between the information and a person, i.e., information "identifiable to an individual."[343] Kang also specifically stated that biometric data constituted personal information about an individual.[344] Clearly, facial recognition software implemented into a wearable computer performs a biometric analysis of a person's face, and thus constitutes personal information under Kang's reasoning- and thus would warrant protection under a privacy law statute. In addition, borrowing from Fourth Amendment case law and Federal and state video voyeurism statutes,[345] an information privacy law should be designed to protect an individual's "reasonable expectation of information privacy" once they enter a public place. While it may be reasonable to expect to be seen

---

[341] *Id*. *See generally* Woodrow Barfield, *Commercial Speech, Intellectual Property Rights, and Advertising Using Virtual Images Inserted into TV, Film, and the Real World*, _ UCLA Entertainment Law Review _ (forthcoming 2006).
[342] Kang, *supra* note 2.
[343] *Id*. at 1206.
[344] *Id*. at 1206-1207.
[345] *See Supra* note 266; *supra* note 269 (Stephanie's Law).

and identified in a public place by individuals who may directly view you, it is unreasonable to expect that you will be filmed, that your recorded image will be uploaded to the internet, and that personal information will be paired to your identity and location. As one aspect of privacy protection in a public place, personal information which may violate a persons privacy if posted on the internet, in a similar manner should also violate a person's information privacy if paired to their image once they entered a public place. This type of information would include not only social security numbers, and medical records, but as noted above, information which could be used to track an individuals movements within public places.

Professor Kang also distinguished between the concepts of "surveillance" and "casual observations," arguing that a law too general might constrain causal observations made in public places, therefore Kang limited his proposed "Information Privacy Act" to cyberspace transactions.[346] As emphasized in this article, video-based wearable computers equipped with facial recognition software and internet capabilities may be used to pair personal information to an individual's image once they enter a public place. Given the capabilities of wirelessly networked wearable computers; an information privacy statute that focused solely on transactions in cyberspace would be too limited in scope to account for the realities of current wearable computing and internet technology. It is the combination of an image being recorded in a public place and having the image paired to information derived from the internet as well as tracking information that must be accounted for in an information privacy statute directed at wearable computers.

A comprehensive information privacy statute should provide for an enforcement mechanism which would establish sanctions against violators and offer redress for

[346] Kang, *supra* note 2, at 1268-1269.

aggrieved individuals. Most effective would be legislation providing a private right cause of action for aggrieved individuals. Further, the statute should be designed to include an exemption for law enforcement who may need to use wearable computer technology to identify individuals and track their movements.[347] And individuals with wearable computers that desire to film individuals in public places, should in some way provide a warning to individuals that they are being filmed, especially if the wearable computer has internet capabilities and the individuals image may be uploaded to the internet. Here the law would need to distinguish between what one would consider "background characters" in the video versus the subject of the filming. It would be onerous and unworkable to expect an individual to warn every potential person captured within the field of view of a camera lens that they were being filmed. In lieu of personally contacting each individual, perhaps the wearable computer itself could effect a warning, possibly in the form of an "on light" to indicate the individual was filming. A statute to account for the capabilities of wearable computers may also be written such that those individuals whose image is analyzed by facial recognition software must provide consent to being filmed in a public place if their image will be uploaded to the internet. Along these lines, given the reported benefits of wearable computers, for example, monitoring a person's medical status or identifying the location of one's kids, a person should have the ability to "opt in" and decide which personal information should be collected and who should be able to view it.[348] If a person does "opt in" for certain applications, the

[347] An interesting question for courts to decide will be whether the increased capabilities of wearable computers to analyze an image, track an individual, and access information about a person from the internet constitutes a search under the Fourth Amendment thus necessitating a warrant before such technology is used by the police.

[348] Schwartz, *supra* note 336.

information privacy statute should prohibit the interception and use of the wireless signal by a third party for uses that violates an individual's information privacy.

In summary, the basic components of an information privacy statute designed to account for the capabilities of wearable computer technology should address the ability to analyze and recognize faces, post facial images on the internet, pair personal information to the posted image, and track an individual's movements in a public place.

VII. CONCLUSIONS

We live in a society where there is a shrinking level or personal privacy. For example, for a small price, one can purchase a month's worth of call information for just about anyone.[349] These are very personal and private records of who an individual calls, when the call was made, and how long was spent on the telephone call. Similar levels of detailed private information can be accessed on the internet for either a small fee or for free. Even with such intrusive practices, wearable computers may result in an even greater loss of personal privacy than has occurred from use of the internet.[350] Therefore, legislatures should address the privacy concerns that result from wearable computers, before the wearable computer technology develops even further to monitor and track individuals in public places.

It should be noted that whether the use of technology which can record images and upload them to the internet, such as cell phones and video-based wearable computers, are desirable technology for a particular community is not only a question of law but also

---

[349] Jeremy Reimer, U.S. Lawmakers Discuss Banning Sales of Phone Logs, most cell phones sold during the last few years are also "E911 capable," meaning that they come equipped with GPS positioning systems. While this feature makes it easier for law enforcement to track down criminals, it also makes it easier for criminals to track down their victims, and for oppressive governments to keep track of their citizens with Orwellian-like efficiency. *Id. available at* http://arstechnica.com/news.ars/post/20060202-6102.html (last visited Feb. 2, 2006).

[350] Choicepoint, *supra* note 41.

a question of public policy. In that regard, in response to the growing use of cell phones images used for voyeuristic purposes, in West Lothian, Scotland, camera phones are banned at all secondary and primary schools to insure the safety and security of pupils.[351] The policy has been supported by the local teachers' association which fears that video images could be misused by pedophiles.[352] While completing banning a technology at a school may be an appropriate means to solve a societal problem at a local level, in the case of wirelessly networked wearable computers a more comprehensive solution is called for, due to both privacy and safety concerns.

When considering privacy in public places, the Fourth Amendment provides protection of individuals in public places only where they have a reasonable expectation of privacy from government intrusion. What happens when the filming of an individual in a public place is done by a private actor? In this case, the main causes of action stem from the classic article on privacy published by *Warren and Brandeis* in 1890[353] and enumerated specifically in the 1960 article by *Prosser*.[354] Both articles, and the case law presented in this article, highlight the fact that a central feature of privacy, is the notion of having a "reasonable expectation of privacy" in a particular space occupied by a person. However, as many of the cases presented in this article emphasized, once a person places themselves "in public," much of their expectations for privacy disappear. One can ask, is this result still reasonable in an age of wirelessly networked wearable computers equipped with facial recognitions software? While the Supreme Court has stood steadfast to the notion of privacy in a public place depending on a rather restricted view of what

---

[351] *See Pupils Face Camera Phone Ban*, http://news.bbc.co.uk/2/hi/uk_news/scotland/3524913.stm (last visited Jan. 8, 2006).
[352] *Id*.
[353] Warren & Brandeis, *supra* note 19.
[354] Prosser, *supra* note 130.

constitutes a reasonable expectation or privacy, the Federal and many State governments in enacting stricter privacy laws, and enacting new legislature to punish video voyeurism, have indicated a wiliness to expand the range of what constitutes a reasonable expectation of privacy in order to keep pace with technology developments. What is needed now is an ever greater expansion of the notion of what constitutes a reasonable expectation of privacy in public spaces. Currently, there are numerous bills being debated at the state and federal level, on just this topic.[355] Therefore, while the future may be leading to a world where technology will be able to monitor, record, and analyze our every movement in public spaces, it is expected that laws will be enacted to provide some privacy protection, not only from government actors, but public actors as well, hopefully such laws will provide more protection for privacy in public places,[356] and will focus on the capabilities of wirelessly networked wearable computers equipped with facial recognition software and other sensors.

---

[355] *See generally* Florence Olsen, *Debate Continues on Data Privacy Bill*, *available at* http://www.fcw.com/article91504-11-21-05-Print (last visited Feb. 2, 2006); *Sen. Durbin Introduces Cell Phone Privacy Bill*, *available at* http://talkleft.com/new_archives/013743.html (last visited Feb. 2, 2006).

[356] Doug Klunder, ACLU, Seattle, Washington, Personal Interview (Nov. 2005).