New Challenges for Privacy Law:
Wearable Computers that Create Electronic Digital Diaries

Stephen S. Intille, Ph.D. and Amy M. Intille, J.D.
September 15, 2003
MIT House_n Technical Report

Abstract

Wearable computing technology developed and deployed in the next 15 years will create fundamental challenges to personal privacy law. This paper reviews current legal precedents in privacy and surveillance law and identifies some of the issues that courts will inevitably be asked to address. We focus on one particular capability of future mobile computing devices: the ability to act as long-term archiving devices and memory aids by continuously recording everyday experiences from on-body sensors such as cameras and microphones. We discuss how the law and social expectations may need to change to prevent the erosion of privacy protection as the use of wearable computing technology becomes pervasive throughout our society.

1. Introduction

Wearable mobile computers will soon be commonplace. In fact, some forms already are. Many people wear their digital watches continuously. These are simple wearable computers. Others carry their mobile phones with them everywhere, including inside their homes. New phones have touch displays, wireless network data access, and sensors such as position locators, voice recognizers, barcode scanners, and cameras. Some watch computers can collect data from sensors worn on other parts of the body, such as a chest strap heart rate monitor.

New mobile computing devices will have small and ergonomic form factors that permit users to comfortably and effortlessly wear them at all times. Like digital watches today, users will remove the devices only when absolutely necessary, such as when showering. These small wearable devices will be capable of nonstop collection, processing, and archival of information about what the wearer is doing and perceiving. This processing and storage of activity data will enable new communication applications. For example, a wearable computer will be able to act as a "cognitive orthotic" by helping users identify and remember people, places, and things [1, 2]. A wrist-worn computer, for instance, could permit the wearer to easily leave and then receive location-based reminders such as, "remind me to pickup toothpaste next time I'm near the supermarket." The same devices may also be used for entertainment and archival purposes. For example, the wearable could create a diary of images of what the wearer is doing and perceiving each day, where pictures associated with moments in the day that were particularly surprising or startling are automatically flagged [3]. In this paper we focus on privacy challenges raised by the ability of a wearable computer to archive tremendous amounts of digital data at low cost. Researchers are already actively working on developing the hardware and software required to make massive archiving of wearable "digital diaries" possible [4, 5].

Corresponding author: Stephen Intille, intille@mit.edu, House_n, Massachusetts Institute of Technology, 1 Cambridge Center, 4FL, Cambridge, MA 02142, USA

Historically, new technological developments have invaded and eroded privacy rights. For instance, mass production printing, photography, and electronic surveillance have each intruded upon Fourth Amendment privacy [6]. In 1890, Warren and Brandeis published a seminal privacy article recognizing a common-law right to privacy because they were concerned about increasing invasions of privacy by the press. Several Nineteenth Century inventions including faster printing presses and "instantaneous" photographs were of particular societal concern [7]. Technologies such as parabolic microphones, wireless radio transmitters, telephone taps, and miniature television cameras are more recent innovations that have eroded privacy in the last one hundred years [6, 8]. The rapid rise and pervasive use of video surveillance technology is arguably one of the most invasive forms of current technology and, as summarized in this paper, the law affords very little protection from video surveillance privacy invasion.

The ability of the wearable computer to capture and process digital data about a user's experience may have tremendous value to users. However, the ability to constantly and, if desired, secretly record one's sensory experiences using both audio and video sensors raises privacy concerns. Not only can data be collected continuously, it can be archived indefinitely.

This paper analyzes the current state of the law regarding video surveillance and privacy. We discuss how current legal precedents may impact the privacy debate that will be triggered by widespread adoption of wearable computers with video and auditory archiving capabilities. Finally, we discuss how both the law and social expectations may need to change to afford greater privacy protection as the use of data-archiving wearable computers becomes more common.

2. Capturing a comprehensive, electronic diary of activity

People seem to have an innate desire to capture information about what they do and see. Diaries, letters, shelves of books, albums of photographs, scrapbooks, home videos, and web blogs are just some examples of ways that people save memories for later enjoyment and reflection. Until recently the most efficient, cost-effective, and reliable manner to save information was through printed text or photographs. However, as the cost of digital memory drops dramatically, people are beginning to save documents electronically. Not only do electronic documents require less physical space, they can be searched and recalled much more quickly and easily than their paper counterparts. For these reasons, it is not uncommon for owners of digital cameras to archive every picture ever taken and to leave the majority of them in a digital format without ever committing them to print. The primary barrier to electronic storage – cost – is diminishing. In this paper we assume that the cost of electronic storage will continue to drop and that within the next ten years terabyte (TB) storage media will be commonly available.

The question then becomes, why not record and save everything? It will soon be possible for wearable computing devices to create comprehensive digital diaries of their user's lives. These wearable computers will continuously record everything the user sees, hears, and reads. The value of such an experiential memory device was realized as early as 1945 [5, 9, 10]. For less than one terabyte, a user can create a digital diary that includes video, audio, photographic, and document data:

- A continuous, 24-hour video stream of 160 x 120 pixels at 10fps MPEG-4 encoding [1.56GB/day, 570GB/year]
- Continuous, 24-hour audio stream in mp3 format (24000 Hz, 16bit stereo) [.57 GB/day, 210 GB per year]
- One 1024 x 768 pixel image per minute, 24 hours/day with lossy JPEG encoding (e.g. could be a page of a book, a fax, etc.) [.57 GB/day; 210 GB/year]
- One 3MB computer file per hour, 16 hours/day (e.g. could be an electronic text file) [72MB/day; .03GB/year]

Using current compression technology, an entire year of experiences can be archived in 990 MB. Based on current trends, by 2007 a terabyte of storage will be available for less than $300 and the price will continue to drop thereafter. A consumer, therefore, could simply purchase one new terabyte drive per year to retain a complete multi-media record of his or her activity [5].

Why would someone do this? Perhaps the user would like to go back in time and reminisce or inquire about the first time he/she met someone else and what that person did/said, a medical exam and what a physician said, an important meeting at work, or photographs from a special vacation. Or, perhaps the user would like to remember the name of great restaurant visited several years ago, the name of someone met at a party, or a cooking technique explained by a friend the previous month. Because audio can be recorded continuously, the user can create a diary of his/her own thoughts simply by speaking at times when others are not around. The user might wish to revisit the thoughts recorded on a particular day.

To make this vision of continuous data recording possible, wearable computers will need wireless body networks that permit sensor devices such as cameras and microphones to be pinned to the shirt or worn on a wrist and send data without encumbering wires to wearable computer elsewhere on the user's person. Already Bluetooth devices exist that send audio wirelessly from ear-mounted headpieces to mobile phones. Future versions will run for an entire day without recharging or a battery replacement, and many of the sensors will be available in form factors that make them nearly impossible to detect by an uninformed observer.

Wearables will do more than simply collect data. They will process it in real time to infer information about the user's tasks and context. This information will be used to help the user with memory tasks (e.g. face recognition [11] and composing messages [12]) and to provide context-sensitive reminders [13]. The wearables will act as cognitive orthotics that help some people with everyday tasks such as navigating their communities, managing medications, and performing their jobs more effectively.

We assume that in 15 years from the date of this writing (2018), consumers will have access to low-cost, mobile computing devices that can continuously record a multi-media record of user activity for archival. These devices will act as cognitive orthotics: helping people with memory recall and other everyday tasks. Some people may be dependent upon the functionality provided by the devices and hesitant, unwilling, or even unable to turn them off.

This wearable data capture technology will raise difficult privacy questions for our society. Although continuous data recording for personal use of the wearer might be valued, does this compromise the privacy of other people in the user's environment who are also being recorded? Can they be recorded without their consent? What type, location, and timing of data collection will be acceptable given the law and in light of social expectation? We consider some of these issues as we review the origins of privacy law.

3. Scenarios of use

To illustrate the legal challenges raised by wearable computing devices that collect multi-media diaries, consider five hypothetical future scenarios:

Scenario 1: The store. Jim has a vision problem and uses wearable system that consists of a mobile phone computer, a wireless earpiece, and a nearly invisible wireless camera pin. The system continuously collects audio/visual information and saves it to disk. Periodically the computer processes the information and constructs electronic models of Jim's activity. By matching imagery of where Jim has been before with his current situation, the system can provide him with additional audio information that helps him accomplish everyday activities despite his poor eyesight. One day, managers at the supermarket where he shops prohibit him from wearing his system in the store, claiming that he could sell the collected data used for guidance to store competitors. Store managers complain that they cannot tell if he has the system turned on or not.

Scenario 2: A home visit. Nancy has a wearable system that consists of her phone and two miniature wireless pins that record video and audio. Nancy records her life each day and later adds an audio track to the video describing how she was feeling about things. Once a week she spends a little time reflecting upon her past experiences. Revisiting both fun and difficult times gives her perspective on her current life that she finds enjoyable. One day she meets some new friends who invite her to dinner at their house. Everyone is having a great time drinking wine, making jokes, and getting to know each other. Her new friends are unaware that Nancy has an audio-visual recording of the entire event that she plans to keep for the rest of her life.

Scenario 3: Sudden fame. Five years after Nancy met her neighbors and long after they had parted ways, one of the neighbors becomes politically active and runs for Governor. Nancy sees the friend on television and, just for kicks, enjoys a few hours reminiscing about some of their past dinners together. To her surprise, some of the comments the political candidate made at the party cause her to have doubts about his fitness for public office. Nancy contacts a local television station and shares her digital memories. They offer to pay her but she declines the money.

Scenario 4: A neighborhood watch. Jim and Nancy live in the same neighborhood and belong to the local neighborhood watch program. They are concerned about a few members of the community who are known pedophiles, and they want to keep tabs on those people. Their wearables use face recognition software and share data with other members of their watch group anytime a person they consider suspicious or a troublemaker is spotted. Jim and Nancy do not need to know who all the

people are, because it all happens behind the scenes. In some cases detailed maps of a person's whereabouts can be constructed, and as more people get wearables and join the maps are getting more detailed all the time. Just for kicks, Jim sometimes sees how much information he can get on the whereabouts of his neighbors, whom he has never met.

Scenario 5: Confiscation. One day Jim is arrested for smoking marijuana and police confiscate his wearable. They search his multi-media diary and discover that three years ago he hit a neighbor's dog while driving and did not report it.

Beginning with Warren and Brandeis's 1890 article recognizing a common-law right of privacy, American privacy law has evolved from several distinct legal areas including "tort law, constitutional law, criminal procedure, civil procedure, family law, and contracts" [14]. These multiple sources and the difficulty in defining "privacy" have caused confusion for the judiciary, commentators, and scholars. In large part, privacy law is slowly evolving (and many would argue eroding) in reaction to the introduction of new technologies [15, 16]. The new capabilities of wearable recording devices will contribute to this evolution, providing new challenges for courts and legal scholars.

In the remainder of this paper we provide historical context within which to consider how courts may approach the issues raised by the five scenarios and similar situations created by the widespread use of wearable technologies with continuous digital recording capabilities. In doing so, we raise more questions than we answer.

4. History of right of privacy law

Privacy law today can be divided into four areas: common-law tort privacy, First Amendment rights and privacy, Fourth Amendment privacy, and fundamental decisional rights privacy [6].

4.1. Common-law right of privacy

Warren and Brandeis were the first legal scholars to introduce a comprehensive notion of a common-law right of privacy into American jurisprudence. Privacy-related notions such as trespass, protecting property from invasion, and individual protections in criminal law already existed as integral parts of early American law [6]. The Warren and Brandeis privacy article, however, marked the first attempt to identify an explicit right of privacy under tort common law. A tort is a wrongful act other than a breach of contract for which relief may be obtained in the form of damages or an injunction. Warren and Brandeis defined this privacy as a right to "be let alone" [7], citing a group of cases from American, English, and Irish courts. They argued that "political, social, and economic" changes in society require recognition of new rights and that the common law will adapt to accommodate those societal needs [7]. Specifically, the rise of an invasive newspaper business and the technological invention of "instantaneous" photographs served as the societal impetus for a right of privacy. They contended that these changes required recognition of a personal right of privacy under American common law.

The new technology of "instantaneous" photographs, in particular, were said to encroach upon the right to "be let alone." In one highly publicized case, two photographers surreptitiously photographed an actress appearing on stage in tights, a scandalous event at the time. Warren and Brandeis warned that, "numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops'" [7]. Only after 30 years of debate did most jurisdictions accept this common-law right of privacy. The first Restatement of Torts recognized this common-law right in 1939 [17]. In an influential 1960 article, Prosser argued that the invasion of privacy tort, designed by Warren and Brandeis, was actually comprised of four distinct categories of tort privacy: (1) intrusion upon seclusion, (2) public disclosure of private facts, (3) false light, and (4) appropriation [17]. Digital archiving via mobile computing devices will lead to challenges in each of these areas.

4.1.1 Intrusion upon seclusion tort

The first area, *intrusion upon seclusion*, overlaps with the torts of trespass and intentional infliction of emotional distress [17, 18]. Prosser derived two limiting factors from the case law that would separate tortious intrusion from non-tortious intrusions. First, a reasonable person must find the intrusion offensive or objectionable. Second, the intrusion must be into something private in nature [17].

Consider Scenario 2. In this situation, is Nancy's recording of her friends in their own home for her own personal diary offensive and objectionable to a reasonable person? Clearly, the answer to this question depends upon the public's general awareness of the use and capabilities of wearable technology. If Nancy's friends have wearables themselves or use hidden miniature cameras in their own home, they are less likely to find Nancy's behavior objectionable. Even if they find Nancy's data recording objectionable, is the intrusion private in nature?

When determining if an intrusion is private in nature, Prosser drew a strong distinction between protection in a private location and a lack of protection in public spaces. For instance, taking a photograph of a person in a public place or on a public street would not qualify as actionable under the privacy tort of intrusion [17].

The conclusion that there can be no intrusion of privacy in a public place rests on two premises. First, a person effectively assumes a risk of scrutiny when entering a public place. Second, there is no distinguishable difference between merely observing a person and taking the person's photograph [19]. A famous case, Gill v. Hearst Publishing Company, supported these premises. A photographer took a photograph of a couple in a romantic pose at the Farmers' Market in Los Angeles. The couple asserted that the photograph published in a magazine without their consent violated their right of privacy. The Gill court decided that the couple waived their right of privacy when they voluntarily assumed an amorous pose in a public setting. 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 then had actually witnessed it at the time of occurrence" [20].

Recently legal scholars have noted that new miniature cameras being used by video voyeurs in public spaces (e.g. to peer up women's dresses) require that the courts acknowledge greater expectation of privacy in the public space [21]. Although people in public spaces assume a risk of scrutiny, they do not expect that scrutiny to include views not possible with the human eye. Further, they do not expect that behavior in the public space can be aggregated to form a more complete record of behavior than possible through a single observation. One could argue that because continuously acquired audio-visual data can be instantly archived forever, shared with others, and used by computers to infer information about another person's behavior, that there is a fundamental difference between visual observation and wearable digital archiving.

In Scenario 2, Nancy is within the home of her guests, not in a public space. Many states have begun to use tort intrusion law to criminalize home voyeurism, where a person views activity in another home without being invited in. Trespass is an element of most of these laws, but in some states "naked eye viewing that does not involve physical intrusion into constitutionally protected areas can be a crime" [16]. Nancy was not trespassing, since her guests invited her in. The physical trespass requirement is likely to written out of the laws as state laws are rewritten to prohibit "peeping toms" from home invasion with new technologies [16]. These laws, however, deal with acts such as viewing naked individuals, not viewing people who have voluntarily invited one inside their home for a causal dinner party.

Video recording and video surveillance in a public space, like photography, does not meet the first element of the privacy intrusion tort. Thus, video surveillance in a public sphere would not be actionable under the privacy tort of intrusion upon seclusion [19]. Like video surveillance in the public sphere, the use of wearable computers within a public area would offer little privacy protection to an individual under the privacy intrusion tort. Under an analysis of the Gill decision, a person appearing in a public space voluntarily waives their right of privacy as to their actions in the public sphere. If a wearable computer's video camera records a person in a public location, this recorded video does not disclose anything private. The only privacy protection that the individual maintains under the intrusion tort against the wearable computer's videotaping capability is based on whether a particular use of the wearable computer would be "highly offensive to a reasonable person" [22]. Given the extensive use of cameras and video camcorders in both public places and private locations, a court would probably not consider the use of a wearable computer in a public space to be highly offensive under a reasonable person standard. This is particularly true for the use of wearable computers when the video camera attachment is obvious to the human eye. Existing law offers little insight into whether the aggregation of data collected in a public sphere by multiple individuals would be considered to reveal private information.

4.1.2 Public disclosure of private facts tort

The second privacy tort *of public disclosure of private facts* also draws a distinction between public and private facts [17]. The public disclosure of embarrassing private facts, similar to intrusion, requires intrusion into something that is secret, secluded, or private. This is measured using standards of what would be offensive and objectionable to a reasonable person. Unlike the intrusion tort, however, disclosure depends upon "publicity." "Publicity" occurs when a matter is communicated in a manner that

is substantially certain to become a matter of public knowledge [22]. This tort can be in conflict with the First Amendment's protection of freedom of the press. Courts will often strike that balance in favor of the First Amendment's highly protected freedom of the press based on a "newsworthyness" test [18].

The question raised by this privacy tort is illustrated by Scenario 3. Nancy used her wearable to record her interactions with someone prior to that person's business becoming a matter of public knowledge. Unlike verbal anecdotes that people know tend to become unreliable over time, Nancy's digital record is seen as difficult to forge and a reliable record of what actually occurred. At the time the material was recorded, it was not newsworthy. However, at the time it is released, it may be. Courts will need to determine if the information about a person's whereabouts from Scenario 4 is communicated in a manner substantially certain to become public knowledge.

4.1.3 Publicity that places a person in a false light

Prosser's third privacy tort consisted of *publicity that places a person in a false light*, which guards against an objectionable false portrayal of a person [17]. Prosser noted two typical false light circumstances: a publisher uses a person's picture to illustrate a book or article when that person has no connection with the article, and a police department includes a non-convicted person's name, photo, and fingerprints among a group of convicted criminals. Prosser observed that the false light tort overlapped greatly with defamation. Wearables with continuous recording are probably less likely to lead to distorted publicity for any given moment, although given the massive amount of information a wearable might collect on someone, snippets of that complete record could be compiled to create a false impression. One reason that people may want to use wearable recording devices is as protection against other people using recording devices that may show them in a false light [23].

4.1.4 Appropriation

The fourth privacy tort, *appropriation*, prohibits the unlawful use of a person's name or identity for a defendant's benefit or advantage [17]. This fourth tort of invasion differs significantly from the other three torts because appropriation deals with a proprietary interest as opposed to a personal privacy interest. This privacy tort often assists celebrities in protecting the commercial value of their "right of publicity" [18]. This tort would make it difficult for Nancy to profit from the digital diary she captured if her profit depended in large part on information acquired about specific people who she had recorded.

Drafters of the Restatement (Second) of Torts subsequently incorporated Prosser's four privacy tort definitions into the Restatement's privacy sections. Courts in at least twenty-eight states have recognized Prosser's four torts, and many courts have adopted language directly from the Restatement sections [19, 22].

4.2. First Amendment rights and privacy

The second major area of privacy law is defined by the First Amendment's Freedom of Speech and Freedom of the Press Clauses. The Free Speech Clause has collided with privacy interests in several

different situations, including instances when door-to-door solicitors communicate with reluctant listeners in their homes. Courts have routinely balanced privacy rights against the Free Speech Clause, which has led to the development of a First Amendment privacy [6].

The Freedom of Press Clause conflicts with privacy rights in cases, for example, where a newspaper published the name of a rape victim who wanted to protect her anonymity. These particular privacy interests in the free press area are classified as privacy torts. Constitutional free press claims generally outweigh common-law privacy tort claims when the two competing interests are balanced against each other [6].

4.2.1 Privacy and free speech

The origins of First Amendment privacy are not clear. This privacy may have been derived from the First Amendment, the Fourth Amendment's "home is your castle" privacy right, common-law right of privacy, or a combination of these three sources. Although the provenance for First Amendment privacy is ambiguous, the Supreme Court has established a privacy "right to be let alone" within the First Amendment by balancing competing privacy and free speech rights [6].

In the 1930s, the notion of First Amendment privacy surfaced in a series of cases involving door-to-door solicitations, setting solicitors' freedom of speech rights against homeowners' interest in privacy at home. The Supreme Court has balanced these conflicting interests and distinguished between commercial solicitation and non-commercial solicitation for religious and political purposes, concluding that commercial solicitation invades personal privacy and that non-commercial solicitation is a protected form of speech [24].

The Supreme Court has favored privacy interests over free speech particularly when the privacy interest is associated with the home [24]. For example, In Martin, Justice Murphy, in a concurring opinion, found an explicit right of privacy in the home stating, "[f]ew, if any, believe more strongly, in the maxim, 'a man's home is his castle,' than I" [25]. The Court's balancing of privacy interests against free speech in locations separate from the home varies greatly in a series of "captive audience" cases [24]. The Court developed the idea that the privacy interest protected by the Free Speech Clause includes a "freedom of the citizen to think and engage in private thoughts, free from the clutter and bombardment of outside speech" [6]. The Supreme Court has upheld the right of people to be insulated from offensive mailings in the home [26] or offensive, "loud and raucous" noises emitted from loudspeakers on the street [27].

Although the precise source for privacy rights for individuals at home or in public is unclear, privacy rights receive quasi-constitutional treatment in the free speech area when privacy rights are balanced against the First Amendment's Free Speech Clause. When state action is involved in the free speech area, privacy rights originate directly from the First and Fourth Amendments [6]. When a private citizen's free speech threatens another person's solitude and free thought, however, tort law and common-law notions protecting individual solitude are the source for privacy rights.

4.2.2 Privacy and free press

Unlike privacy interests in the free speech area, which have received quasi-constitutional treatment, privacy rights in the free press area are derived from common-law privacy torts, which are outside the perimeter of Constitutional protection. Generally, when courts balance privacy interests against Free Press rights, courts tip the balance in favor of freedom of the press [6].

The public disclosure privacy tort, as it appears in the Restatement (Second) of Torts, limits liability to situations where the publication would be "highly offensive to a reasonable person" and the publicized matter was not of "legitimate concern to the public" [22]. A "newsworthiness" privilege is extended to the public disclosure tort, allowing the publishing of private information and limiting it only when the published information ceases to inform and it becomes "morbid and sensational prying." In addition to the privacy tort's newsworthiness limitation, media defendants possess an even stronger defense against privacy claims through First Amendment case law [28].

In the 1960s, the Supreme Court began forming a protective structure for free press rights in a line of defamation cases that broadened constitutional protection of false and defamatory speech [29]. False speech involving a matter of public interest is protected speech under the First Amendment, unless a plaintiff proves knowledge of falsity or reckless disregard for the truth by the media defendant [28].

While truthful speech by definition is not defamatory, truthful speech by the press can invade personal privacy. The Supreme Court has virtually eliminated the possibility of recovery against a truthful speech invasion of privacy under the public disclosure tort claim [29].

Unlike the public disclosure privacy tort, the intrusion privacy tort continues as a viable claim against an invasive media defendant [28]. The intrusion privacy tort protects against a "physical intrusion . . . upon the solitude or seclusion . . . or . . . private affairs," whereas the public disclosure privacy tort protects against publicity of a person's "private affairs" [22]. The "newsworthiness" privilege does not apply in the intrusion upon seclusion privacy action because publicity is not an element of the tort. Additionally, First Amendment protection is not applicable in this area. Thus, the absence of the First Amendment and "newsworthiness" limitations upon the intrusion tort provides a potential avenue of recovery for plaintiffs when the public disclosure tort rarely survives a First Amendment Free Press challenge [22, 28].

4.3 Fourth Amendment privacy

The Supreme Court linked privacy to the Fourth Amendment in its 1886 decision in Boyd v. United States, connecting the privacy idea of "home is your castle" to the Fourth Amendment [30]. Later, in Olmstead v. United States, Brandeis grafted his idea of a "right to be let alone" onto the Fourth Amendment's search and seizure law [31]. Concerned about rapid technological advancements such as wiretapping of telephone lines at issue in Olmstead, Brandeis argued for an expansion of the test that looked strictly for physical trespass in search and seizure of tangible property [6].

Following the Olmstead decision, Fourth Amendment law changed only gradually to protect privacy interests up until the Court's landmark decision in Katz v. United States in 1967 [6, 32]. Before Katz, the cases that followed Olmstead clung to the notion that no illegal search and seizure occurred unless a court found evidence of physical trespass on protected property or seizure of tangible goods [24]. In Silverman v. United States, the Court signaled an interest in shifting its focus from the trespass element to whether privacy had indeed been invaded, although it based this decision upon the physical trespass requirement [33].

Although privacy law changed very little through the 1940s and 1950s, surveillance technology developed rapidly both in its availability and technical sophistication [8]. Wide availability of this technology led to a dramatic rise in surreptitious monitoring of individuals by government agents, police, private investigators, and other private citizens. State statutes designed to protect against wiretapping were generally ineffective because of the broad exceptions carved out of these statutes [6]. By the 1960s, overwhelming national concern about unfettered governmental and private surveillance prompted dramatic judicial and legislative changes in the law protecting privacy interests [8].

In 1967, the Court abandoned its adherence to a physical trespass requirement in Katz, deciding that the Fourth Amendment "protects people, not places" [32]. In Katz, the federal authorities attached an electronic listening and recording device to the outside of a public telephone booth, surreptitiously recording Katz's telephone calls in a bookmaking operation. The majority in Katz overruled Olmstead's physical intrusion test and concluded that the Fourth Amendment protects people, rather than physical locations. This is an important finding with respect to wearable computing, since those computers travel with the individual rather than stay in a fixed location. In his concurring opinion, Justice Harlan developed a two-part privacy expectation test that reviews both a subjective expectation of privacy and an objective, reasonable expectation of privacy. Shortly after Katz, the Court in Terry v. Ohio adopted Justice Harlan's reasonable expectation of privacy test under Fourth Amendment case analysis [34]. Almost forty years since Brandeis expressed his concern regarding technology's advancing intrusion upon privacy, the Court provided its strongest measure of protection of Fourth Amendment privacy against encroaching surveillance technologies [6].

Following the Katz decision, the Court has examined the reasonable expectation of privacy in a wide array of cases on an ad hoc basis. In deciding the reasonableness of searches and seizures, the Court has created a hierarchical structure among types of searches that merit protection with a warrant [6]. The Court has found a reasonable expectation of privacy against governmental intrusion in cases involving "bugging devices; administrative searches of homes and businesses; searches of closed luggage and footlockers; sealed packages; beepers . . . inside drums of chemicals . . . border patrol search[es] . . . for illegal aliens; traffic checkpoints searching for concealed aliens; and random spot checks for automobiles to inspect . . . licenses and vehicle registrations" [6]. The Court, however, has decided there is an unreasonable expectation of privacy in cases involving a person's bank records, voice and writing exemplars, pen registers, conversations with wired informants, and closed compartments within automobiles. Although legal scholars argue that, following Katz, the Court has diminished privacy rights under the Fourth Amendment, a balance of privacy interests against unreasonable searches and seizures is firmly entrenched within Fourth Amendment legal analysis. Therefore, Fourth Amendment privacy

can be defined as the "right to be let alone, with respect to governmental searches and seizures that invade a sphere of individual solitude deemed reasonable by society" [6].

Scenario 5, therefore, raises an interesting question because the record that the government might obtain from Jim's confiscated wearable could contain a lifetime of information. Does the government, upon determining they have a right to perform a physical search, thereby have the right to search a record of Jim's entire lifetime of behavior or just some reasonable period of recent history?

The potential utilization of wearable computers by government law enforcement agents would implicate the Fourth Amendment's protection against unreasonable searches and seizures [6]. The Fourth Amendment's protection against unreasonable searches and seizures would govern a law enforcement agency's use of a wearable computer in a criminal investigation. Consequently, courts will apply the Katz reasonable expectation of privacy test in determining a person's privacy rights. Depending upon the context in which the wearable computer is utilized, an individual will be protected from the governmental use of wearable computers in warrantless searches and seizures when a person has a reasonable expectation of privacy. Courts will apply the Katz reasonable expectation of privacy test and subsequent Fourth Amendment case law regarding warrantless searches and seizures to the use of wearable computers as the courts have done in the past with other surveillance tools, including bugging devices and video surveillance.

In a recent decision, Kyllo v. United States, the Court found that surveillance of a home is a search 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" [35]. In other cases, devices that are "in general public use" such as zoom cameras used to peer into homes have been found to not constitute a search [36]. This begs the following question. When wearable experience recorders are in general public use, will law enforcement be able to use networks of wearables, as in Scenario 4, to obtain information?

4.4 Privacy as a fundamental right

One of the most controversial forms of constitutional privacy law originates from the Supreme Court's decision in Griswold v. Connecticut [37]. In Griswold, the Court decided that a state statute prohibiting the use and distribution of contraceptives violated a right to marital privacy. Justice Douglas located the source of this fundamental constitutional right within the "penumbras" of guarantees contained in the First, Third, Fourth, Fifth, and Ninth Amendments. While all the Justices disagreed on the specific constitutional source for this fundamental privacy right, a majority of the Court agreed that a fundamental right of privacy extended to marital decisions within the bedroom [6].

The second major step in the development of fundamental decisional privacy occurred with the landmark case of Roe v. Wade, establishing a constitutional right of privacy that protects a woman's decision to have an abortion [38]. The Court in Roe based this fundamental privacy decision, not on the "penumbral" rights as in Griswold, but on the notion of an ordered liberty in the Fourteenth Amendment. The Court made a bold and difficult jump by focusing upon the provision of constitutional protection for

the privacy of the individual decision-making process [6]. While in Griswold the Court rested privacy protection in the marital bedroom based on a familiar protection of privacy in the home, in Roe the Court departed from its familiar emphasis that protects locational privacy and recognized privacy protection for individual choices.

Through the Griswold and Roe line of cases, the Supreme Court created a constitutional right of privacy protecting fundamental decision-making. Like the development of other areas of privacy law, in these cases the Court was responding to technological advancements that could not have been contemplated during the drafting of the Constitution [6]. Given an evolving notion of "liberty," fundamental decisional privacy will continue to develop in response to changing societal demands. It may be that when wearable devices do become indispensable cognitive aids for people that fundamental decisional privacy will be invoked in situations such as Scenario 1.

4.5 Congressional treatment of video surveillance

In response to the Supreme Court's Katz aural surveillance decision, Congress passed a law requiring law enforcement officials to apply for a court order to intercept communications [39]. Additionally, Title III controls the interception of electronic, wire, and oral communications, but it does not regulate video surveillance [14]. Therefore, some federal courts apply some of Title III's requirements to silent video surveillance, while others find all Title III requirements applicable to video surveillance. Congress has never clarified this issue, so video surveillance continues to be unregulated by Title III although video surveillance is arguably more invasive than audio surveillance [14]. Given the similarities in technology between video camera surveillance and silent video recorded by wearable computers, federal courts are likely to follow case law in Torres and Mesa-Rincon, applying Title III requirements to the use of video surveillance. Therefore, Title III requirements in most circumstances would be applied to the use of wearable computers by government agents in surveillance investigations.

Title III shows the piecemeal fashion in which the courts have dealt with privacy invasion due to new technologies. How current courts would deal with all five wearable scenarios would differ based on weather the wearable user was recording audio, video, or audio and video. To avoid confusion, the courts will eventually be forced to adopt a definition of privacy based on *information* rather than on specific technologies.

4.6 Federal court treatment of video surveillance

Federal courts have taken numerous approaches to granting video surveillance warrants because Title III does not contain regulatory requirements for video surveillance warrants [14]. In United States v. Torres, the Court of Appeals for the Seventh Circuit measured the reasonableness of a video surveillance search by balancing the need for the search against the invasiveness of that search [40]. The Torres court upheld the district court's order allowing surreptitious entries into apartments for the installation of electronic bugs and television cameras to monitor terrorist organizations' building of bombs because the Government demonstrated that the need for the search outweighed its invasiveness. The Torres court, however, recognized the enormously intrusive nature of video surveillance and

cautioned against the strong potential of video surveillance to invade personal privacy. In United States v. Mesa-Rincon, the Court of Appeals for the Tenth Circuit upheld the surreptitious videotaping of a counterfeiting operation in an office building, even though in the process of filming this operation, law enforcement officials observed an unknown male engaged in sexual activity [41]. The Mesa-Rincon court applied Title III's requirements for interception of oral communications, arguing that Title III requirements provided a strong analogy to video surveillance even though video interception can be vastly more intrusive.

5. Wearable computing and privacy law

Wearable technologies will require courts to revisit the decisions described in Section 4 as they confront cases resulting from situations such as those described in the 5 scenarios. Some issues are discussed below.

- Wearables are not tied to a particular location and continuously acquiring data as a user transitions from situation to situation and place to place. Current law has evolved based on technologies that are primarily fixed to particular locations. Wearable technology may force courts to shift the definition of privacy towards one dealing with a person-based rather than a place-based right.
- Wearables will be worn by typical citizens, not just law enforcement officials, reporters, "peeping toms," or celebrities. Nearly all surveillance privacy law deals with one of these four special groups. Widespread adoption of wearables will lead to situations where two non-newsworthy parties are in dispute over the collection of information about situations where neither party has engaged in an act that is as blatantly objectionable as spying on someone who is naked. The privacy intrusions may be subtle and objections to recording may, in large part, result not from the specific material recorded but from the permanent and detailed record that a wearable device will effortlessly create.
- As prices for digital storage drop, not only will it be possible to record terabytes of information but it will also be easier to store it and maintain it indefinitely. When storage is essentially free, why delete any data? Data can be stored for a lifetime. It is the persistent nature of the digital recordings made via wearables that will, in part, make the technology powerful. Privacy law today has evolved around situations dealing with observations made in the moment. The law must evolve to consider situations where data is collected in dramatically different contexts very far apart in time. Some scholars have begun to argue that there is a "distinguishable difference" between observing a person and taking a photograph due to the permanent record of the photograph. Further, one can reasonably argue there is a difference between a photograph and a video, because the video captures more of a person's personality [14]. Extending the analogy further, it seems reasonable to argue that a complete multi-media record acquired over multiple interactions and stored indefinitely is even more potentially invasive.
- As wearables become more powerful, they will also be used as cognitive orthotics – memory aids that are extensions of our minds. Those with disabilities may rely on the devices for everyday tasks such as navigation and health maintenance (e.g. [42, 43]) or for communication (e.g. ASL recognition [44]). Some devices may provide required medical monitoring and

people may not wish or be able to remove them; current pacemakers are versions of simple wearable computers. Thus, the wearable computer's sensing technology assists the user to enhance or augment the user's memory [45]. The devices will be always on, and they can be constructed so that it is impossible for a causal observer to tell if various recording capabilities are functional at any given time.

- Finally, wearables are not isolated devices but will be connected to digital networks and other wearable users. It will be impossible for a casual observer to tell (1) what is being recorded, (2) where it is being sent to, (3) how long it will be kept, and (4) what information it will be correlated with. Information that is collected by an individual may be harmless, but the same information when aggregated with other "harmless" information may enable data mining algorithms to infer details about the lives of people that the wearable user encounters in public spaces. These tracking capabilities, already in use with surveillance cameras, threaten an individual's privacy [14].

6. Ubiquitous surveillance: a present-day exemplar

Ubiquitous video surveillance technology provides anecdotal evidence of how wearable archiving technologies might be received, at least in public spaces. Surveillance cameras are now common in public spaces, including on public streets, in retail stores, in banks, in parking lots, at work, in courthouses, at hotels, at concerts and sporting events, and on school buses. The vast numbers of cameras virtually ensure that some portion of most people's lives are monitored. One study estimated that the average London resident is monitored by 300 different cameras on 30 different networks in a single day [46]. In addition to governmental public street video surveillance systems and private entity security camera systems, the pervasive use of millions of video camcorders by individual people to record the events around them has contributed to the diminished ability for individuals to maintain their personal privacy.

The video camera has been compared to the six-gun of the Wild West, as a "great equalizer," based upon a video camera's ability as a "truth-telling device that can cut through lies" [19]. Proponents of the video camcorder have praised its ability to "empower people" and serve the public good [19, 23]. Well-publicized and notable examples of surreptitious filming serving the public good include George Halliday's videotape of Los Angeles police beating Rodney King, an environmentalist's recording of fisherman killing dolphins caught in tuna nets, and a victim's video used to prosecute the defendant who assaulted him. These instances of positive, surreptitious videotaping, however, are overshadowed by situations when video cameras have intruded unreasonably upon an individual's privacy. Voyeurs have frequently used the video camera to surreptitiously record people in private, intimate settings. Surreptitious video recording has invaded personal privacy in non-voyeuristic contexts as well. For example, other types of invasive secret recording include the following: a university recording of a college coach and athletes to monitor possible rule violations, a police video recording of defendant's meeting with counsel, a business's recording of information regarding competitor's products, and a tabloid news organization's encouragement of amateur video submissions [19].

Surveillance cameras, while disliked by many, have become firmly rooted in our society. They are accepted as a fact of life. Wearable recording devices will explode the number of cameras in public spaces. Will people react differently to the use of these wearable recording devices in public spaces? We do not believe they will.

7. The key role of social convention and expectation

We expect that the greatest challenge raised by wearable computing technology will not be in public spaces but in the home. Scenarios 2 and 3 illustrate the problem. What right to privacy can be expected from members of our family, community, and workplace, particularly when we bring those people into our own homes?

Based on the evolution of privacy law to date, the key factor to consider is the community standard of "reasonable expectation" of privacy. Courts afford a person's home the highest level of privacy protection under the intrusion on privacy tort, but video surveillance in private places receives differing treatment under the privacy intrusion tort depending upon a measure of the reasonable expectation of privacy [17]. How expectation changes over time may ultimately determine how courts interpret the privacy threat of wearable data collectors.

Courts have held that individuals have the strongest reasonable expectation of privacy in their homes. In an employee's office, this reasonable expectation of privacy diminishes because the employee's privacy interests are balanced against the employer's interests in conducting video surveillance [47]. The early-adopter wearable computer user will have to exercise the greatest caution to be certain not to intrude upon the seclusion of people in their homes. Today, for instance, the use of the video camera on a wearable computer in a person's home without notification is likely to be highly offensive to a reasonable person. Wearable computer use is relatively new and unknown to the average person. As the use of wearable computers increases over time and more people become aware of their capabilities, however, the use of the video camera on the wearable computer is less likely to highly offend a reasonable person. In non-private settings, many people have already come to expect and accept video ubiquitous video cameras. Many people find the cameras comforting, knowing that in the event of a crime they may provide additional safety or help to bring a criminal to justice. For public cameras, our society appears to be heading down a path of widespread acceptance.

We believe that it is important for technologists to acknowledge that the expectations people have about privacy will, in part, be established by the early generations of the devices. Do social norms about notification evolve? Is the technology designed to encourage these social norms? If so, people may develop an expectation that they are not being recorded unless told otherwise when in the presence of others. Alternatively, does our society generally assume that anyone can be recording at any time and accept that inconvenience because of the appeal of always-on, digital diaries for personal use? Do people feel the need to "shoot back" and record others in case they are being recorded themselves [23]. In this case, people may assume they are being recorded unless notified otherwise.

The reaction of private business to wearable technology will also influence societal expectation. For instance, will Jim in Scenario 1 be permitted to use his device or will the store attempt to outlaw public use of wearables? If the store does outlaw wearables to try and protect trade secrets, will it unintentionally encourage Jim to invest in hidden wearable recording equipment to subvert the store? Since Jim will use this equipment outside of the store, it may lead his acquaintances to assume they are being recorded unless told otherwise. After all, if people can't remember to turn off their mobile phones, why should we trust them to turn off their hidden recording devices, even if they meant to do so?

Certainly for some time people will not have the expectation that everyday conversations are being recorded, but what will happen in 20 years? "Nanny cams" have only been widely available and inexpensive for several years. Still, it would already be somewhat naïve for a nanny to dismiss the possibility that his or her employer has hidden recording devices. The popularity of nanny cams shows that expectations can change rapidly. Further, even parents who would have an aversive reaction to being recorded at their own workplace will consider recording a nanny for the protection of their child.

8. Conclusion

As Warren and Brandeis predicted in their 1890 article, new electronic surveillance technologies over the last one hundred years have greatly reduced a person's "right to be let alone." Pervasive societal use of video surveillance technologies has virtually eliminated any expectation of privacy in public locations, while video surveillance systems in private spaces continue to encroach upon privacy rights. Like video surveillance systems, wearable computers represent a new threat to privacy rights because these powerful new tools can constantly record and store everything about a user's environment through sensors. Although wearable computers are a relatively new technology, the wearable computer will become a pervasive tool used by almost all computer users in the near future.

Currently, there are no statutes or decisions directly regulating a wearable computer's intrusion into personal privacy rights. Yet, inevitably the wearable computer's ability to record video and audio communications will encroach on individual's privacy. Current laws governing video surveillance technology's intrusion with privacy rights provides a good starting point to analyze and resolve the conflict between ubiquitous wearable computer use and protecting personal privacy rights.

References Cited

[1] R. Levinson, "The planning and execution assistant and trainer (PEAT)," *The Journal of Head Trauma Rehabilitation*, 1997.

[2] C. E. McCarthy and M. E. Pollack, "A plan-based personalized cognitive orthotic," in *Proceedings of the Sixth International Conference on Artificial Intelligence Planning Systems*, M. Ghallab, J. Hertzberg, and P. Traverso, Eds.: AAAI Press, 2002, pp. 243-252.

[3] J. Healey and R. Picard, "StartleCam: a cybernetic wearable camera," in *Proceedings of the Second International Symposium on Wearable Computers*: IEEE Press, 1998, pp. 42-49.

[4] B. P. Clarkson and A. Pentland, "Unsupervised clustering of ambulatory audio and video," in *Proceedings of the 1999 IEEE International Conference on Acoustics, Speech and Signal Processing*, vol. 6: IEEE Press, 1999, pp. 15-19.

[5] J. Gemmell, G. Bell, R. Lueder, S. Drucker, and C. Wong, "MyLifeBits: fulfilling the Memex vision," in *Proceedings of ACM Multimedia '02*: ACM Press, 2002, pp. 235-238.

[6] K. Gormley, "One hundred years of privacy," *Wisconsin Law Review*, vol. 1992, pp. 1335, 1992.

[7] S. D. Warren and L. D. Brandeis, "The right to privacy," *Harvard Law Review*, vol. 4, pp. 193, 1890.

[8] A. F. Westin, *Privacy and Freedom*, 1st ed. New York,: Atheneum, 1967.

[9] D. Norman, *Turn Signals are the Facial Expressions of Automobiles*: Addison Wesley, 1992.

[10] V. Bush, "As we may think," in *The Atlantic Monthly*, vol. 176, 1945, pp. 101-108.

[11] A. Pentland and T. Choudhury, "Face recognition for smart environments," *IEEE Computer*, vol. 33, pp. 50-55, 2000.

[12] B. Rhodes and P. Maes, "Just-in-time information retrieval agents," *IBM Systems Journal*, vol. 39, pp. 685-704, 2000.

[13] G. D. Abowd, A. K. Dey, R. Orr, and J. Brotherton, "Context-awareness in wearable and ubiquitous computing," in *Proceedings of the First International Symposium on Wearable Computers*: IEEE Press, 1997, pp. 179-180.

[14] Q. Burrows, "Scowl because you're on Candid Camera: privacy and video surveillance," *Valparaiso University Law Review*, vol. 31, pp. 1079, 1997.

[15] B. Barr, "Legislative reform commentaries: a tyrant's toolbox: technology and privacy in America," *J. Legis*, vol. 26, pp. 71, 2000.

[16] C. Slobogin, "Modern studies in privacy law: searching for the meaning of fourth amendment privacy after Kyllo v. United States," *Minnesota Law Review*, vol. 86, pp. 1393, 2002.

[17] W. L. Prosser, "Privacy," *Califorina Law Review*, vol. 48, pp. 383, 1960.

[18] E. Alderman and C. Kennedy, *The Right to Privacy*, 1st ed. New York: Knopf, 1995.

[19] A. J. McClurg, "Bringing privacy law out of the closet: a tort theory of liability for intrusions in public places," *North Carolina Law Review*, vol. 73, pp. 989, 1995.

[20] "Gill v. Hearst Publishing," in *P.2d*, vol. 253: California, 1953, pp. 441.

[21] L. E. Rothenberg, "Comment: re-thinking privacy: peeping toms, video voyeurs, and failure of the criminal law to recognitze a realistic expectation of privacy in the public space," *Am. U. L. Rev*, vol. 49, pp. 1127, 2000.

[22] *Restatement (Second) of Torts*, 1976.

[23] S. Mann, "Privacy Issues of Wearable Cameras Versus Surveillance Cameras," 1995.

[24] D. M. O'Brien, *Privacy, law, and public policy*. New York, N.Y.: Praeger, 1979.

[25] "Martin v. City of Struthers," in *U.S.*, vol. 319: U.S. Supreme Court, 1943, pp. 141.

[26] "Rowan v. United States Post Office Dep't," in *U.S.*, vol. 397: U.S. Supreme Court, 1970, pp. 728.

[27] "Kovacs v. Cooper," in *U.S.*, vol. 366: U.S. Supreme Court, 1949, pp. 77.

[28] E. W. Gonzales, "Get that camera out of my face! An examination of the viability of suing "tabloid television" for invasion of privacy," *University of Miami Law Review*, vol. 51, pp. 935, 1997.

[29] P. B. Edelman, "Free press v. privacy: haunted by the ghost of Justice Black," *Texas Law Review*, vol. 68, pp. 1195, 1990.

[30] "Boyd v. United States," in *U.S.*, vol. 116: U.S. Supreme Court, 1886, pp. 616.

[31] "Olmstead v. United States," in *U.S.*, vol. 277: U.S. Supreme Court, 1928, pp. 438.

[32] "Katz v. United States," in *U.S.*, vol. 389: U.S. Supreme Court, 1967, pp. 347.

[33] "Silverman v. United States," in *U.S.*, vol. 365: U.S. Supreme Court, 1961, pp. 505.

[34] "Terry v. Ohio," in *U.S.*, vol. 392: U.S. Supreme Court, 1968, pp. 1.
[35] "Kyllo v. United States," in *U.S.*, vol. 533: U.S. Supreme Court, 2001, pp. 27.
[36] "State v. Vogel," in *N.W.2d*, vol. 428: S.D., 1988, pp. 272.
[37] "Griswold v. Connecticut," in *U.S.*, vol. 381: U.S. Supreme Court, 1965, pp. 479.
[38] "Roe v. Wade," in *U.S.*, vol. 410: U.S. Supreme Court, 1973, pp. 113.
[39] "Title III of the Omnibus Crime Control and Safe Streets Act of 1968," in *U.S.C.*, vol. 18, 1994.
[40] "United States v. Torres," in *F.2d*, vol. 751: 7th Cir., 1984, pp. 875.
[41] "United States v. Mesa-Rincon," in *F.2d*, vol. 911: 10th Cir., 1990, pp. 1433.
[42] S. Ertan and a. others, "A wearable haptic navigation guidance system," in *Proceedings of the Second International Symposium on Wearable Computers*: IEEE Press, 1998, pp. 164-165.
[43] S. Ram and J. Sharf, "The People Sensor: a mobility aid for the visually impaired," in *Proceedings of the Second International Symposium on Wearable Computers*: IEEE Press, 1998, pp. 166 -167.
[44] T. Starner and A. Pentland, "Real-time American Sign Language recognition from video using hidden Markov models," in *Proceedings of the International Symposium on Computer Vision 1995*: IEEE Press, 1995, pp. 265-270.
[45] B. J. Rhodes, "The Wearable Remembrance Agent: a system for augmenting memory," in *Proceedings of the First International Symposium on Wearable Computers*: IEEE Press, 1997, pp. 123-128.
[46] D. Gadher, "Smile, you're on 300 Candid Cameras," in *Sunday Times (London)*. London, 1999.
[47] R. G. Boehmer, "Artificial monitoring and surveillance of employees: the fine line dividing the prudently managed enterprise from the modern sweatshop," *DePaul Law Review*, vol. 41, pp. 739, 1992.