Summer 2006

No Direction Home: Will the Law Keep Pace With Human Tracking Technology to Protect Individual Privacy and Stop Geoslavery

William A. Herbert

No Direction Home: Will The Law Keep Pace With Human Tracking Technology to Protect Individual Privacy and Stop Geoslavery?

WILLIAM A. HERBERT*

ABSTRACT

Increasingly, public and private employers are utilizing human tracking devices to monitor employee movement and conduct. Due to the propensity of American labor law to give greater weight to employer property interests over most employee privacy expectations, there are currently few limitations on the use of human tracking in employment. The scope and nature of current legal principles regarding individual privacy are not sufficient to respond to the rapid development and use of human tracking technology. The academic use of the phrase "geoslavery" to describe the abusive use of such technology underscores its power. This article examines the use of such technology under current federal and state law and suggests potential means for developing greater legal protections against the abusive use of the technology and the intrusion into personal privacy.

INTRODUCTION

The creation and increased use of various forms of human tracking technology by governmental entities, private entities and individuals raise profound policy and legal issues for our society. The scope of constitutional, legislative or administrative limitations on the use of such technology reflects on our society's concepts of freedom, individual autonomy, and protected privacy. As technology advances, it expands the means for privacy intrusions, thereby limiting the personal secrets and confidences that can be concealed. New technological tools diminish the ability of individuals to maintain a protected zone against physical, sensational, informational, and cyber intrusions. The growing availability and use of human tracking technology diminishes privacy interests that may precipitate societal demands for increased legal protections.

How freedom and privacy are defined today has substantive consequences in the legal measures that will be devised and applied to

* Senior Counsel, CSEA Local 1000 AFSCME, AFL-CIO, Albany, New York, Herbert@cseainc.org. An earlier version of this article was presented at the 2006 Annual Meeting of the American Association for the Advancement of Science in St. Louis.

protect those interests. As Columbia University historian Eric Foner has shown, the concept and boundaries of freedom have changed over the course of American history. Throughout our history, the definition of freedom has been constantly redefined but has always been subject to a balance between individual rights and property rights, as well as a balance between the right of the individual and the power of the state.[1] Similar balances are applicable in how the contours of protected individual privacy are defined.

In order to respond to the power of contemporary human tracking, a new societal consensus needs to be reached regarding what constitutes privacy and how it can be protected. At the same time, a judgment must be reached regarding whether the legal standards applicable to government surveillance under the Constitution should be the same for non-governmental surveillance.

In contemporary American culture, some view the concept of freedom as being manifested in consumerism, with the ubiquitous cell phone as a primary symbol. It is doubtful that most cell phone users are aware that the same technology that grants them this sense of consumer freedom, also results in wireless companies receiving automatic and continuous updates regarding their location.[2] Physical possession of a cell phone renders an individual vulnerable to location surveillance by government entities. When an employer distributes a cell phone for use by an employee, the employee's location becomes subject to location monitoring by the employer on and off the job. A third party who obtains physical access to another person's cell phone can easily transform it into a stalking device by registering it with an internet location based service.[3] Mass recognition of this non-negotiated trade of a cellular sense of freedom for perpetual

---

[1] ERIC FONER, THE STORY OF AMERICAN FREEDOM (1998).

[2] It is even less probable that cellular customers know or understand the Wireless Communications and Public Safety Act of 1999 which places certain restrictions on the use and disclosure of customer location information. 47 U.S.C. § 222 (2006). The Federal Communication Commission's 2002 denial of a petition filed by an industry group and supported by privacy advocacy groups seeking commencement of rulemaking to clarify the statute's privacy provisions increased the likelihood of public ignorance or misunderstanding regarding the statute's location information protections. *In the Matter of* Request by Cellular Telecommunications and Internet Association to Commence Rulemaking to Establish Fair Location Information Practices F.C.C. 02-208 (2002), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-02-208A1.pdf.

[3] Ben Goldacre, *How I Stalked My Girlfriend*, GUARDIAN, Feb. 1, 2006, http://technology.guardian.co.uk/print/0,,5388423-117802,00.html (last visited May 12, 2006).

surveillance may constitute an Achilles heel to the currently unregulated location based tracking marketplace.

Unlike the debates connected with bioethics and stem cell research, the legal and ethical issues connected with human tracking technology have not been subjected to a serious and rigorous debate. Whether our society is prepared to collectively accept narrow notions of privacy and autonomy through electronic location devices remains to a large extent unexplored. Media disclosures of unchecked and possibly unlawful use of presidential authority to engage in warrantless technologically-based surveillance of Americans may spur a more reasoned and spirited societal discussion regarding the impact of new technology on personal privacy.[4] Such disclosures may render useless the political cliché "9/11 changed everything" as justification for the erosion of protected privacy interests and other civil liberties.[5] It remains to be seen whether the discussion regarding unchecked presidential power will extend to a broader questioning of various forms of electronic surveillance.

This article will discuss various legal principles and issues associated with the use of the following human tracking technologies: global positioning system (hereinafter "GPS"),[6] radio frequency

---

[4] Leslie Cauley, *NSA has Massive Database of Americans' Phone Calls*, USA TODAY, May 11, 2006, *available at* http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm; James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1; Eric Lichtblau & James Risen, *Spy Agency Mined Vast Data Trove, Officials Report*, N.Y. TIMES, Dec. 24, 2005, at A1; Matthew L.Wald, *Widespread Radioactivity Monitoring Is Confirmed*, N.Y. TIMES, Dec. 24, 2005, *available at* http://www.nytimes.com/2005/12/24/national/24radioactive.html?ex=1293080400&en=0d3801d05367f8c0&ei=5088&partner=rssnyt&emc=rss.

[5] JEFFREY ROSEN, THE NAKED CROWD: RECLAIMING SECURITY AND FREEDOM IN AN ANXIOUS AGE 55-61 (2004) [hereinafter NAKED CROWD]. Among the many questionable uses of the September 11, 2001 tragedy as a rationale for policy changes was the 2004 National Labor Relations Board's decision that cited 9/11 as justification for overturning prior precedent that had recognized a statutory right of a private sector employee in an unorganized worksite to be represented by a co-worker during a disciplinary interrogation. IBM Corp., Cases 11-CA-19324, 11-CA-19329, 11-CA-19334, 341 N.L.R.B. No.148, 2004 WL 1335742 (2004).

[6] GPS is a satellite-based electronic system that provides very precise tracking of objects, individuals, and other animals in real time anywhere on the planet. Originally developed by the military, GPS technology has been available for civilian use for over twenty years. Through triangulation of information from satellite signals, a GPS receiver can determine the speed, latitude, and longitude of an object or individual under surveillance. GPS receivers can be attached or installed in objects such as vehicles, cell phones, and laptops. In addition, GPS receivers can be carried by, attached to, or implanted in an individual. April A. Otterberg, *GPS Tracking Technology: The Case for Revisiting Knotts and Shifting the Supreme Court's Theory of the Public Space Under the Fourth Amendment*, 46 B.C.L. REV. 661, 665-666

identification (hereinafter "RFID"),[7] cellular technology,[8] and biometrics[9] in the public and private sectors. In addition, it will suggest potential solutions aimed at creating a balance between liberty and security as they relate to the utilization of human tracking devices. The application of such principles and the nature of the solutions will depend on the type of tracking device and the context in which the device is utilized. For example, the legal rules applicable to mandatory or voluntary human implants containing location technology should be far more restrictive than limitations placed on an employer utilizing a location device to track an employee driving an employer owned vehicle during working hours.[10] Concerns relating to privacy and

---

(2005); Kristin E. Edmundson, *Global Positioning System Implants: Must Consumer Privacy Be Lost In Order for People to be Found?*, 38 IND. L. REV. 207, 209-212 (2005).

[7] RFID is a radio-based identification system that utilizes tags with computer chips containing digital information that can be used to track and identify humans, animals, and inanimate objects. The digital information contained in the microchip can be read through the use of an RFID reader. There are two types of RFID tags. An active RFID tag is battery powered and emits a regular signal. In contrast, a passive RFID tag is powered only when in contact with a reader. D. Zachary Hostetter, *When Small Technology is a Big Deal: Legal Issues Arising from Business Use of RFID*, 2 SHIDLER J. L. COM. & TECH. 10 (2005), *available at* http://www.lctjournal.washington.edu/Vol2/a010Hostetter.html. Common uses of RFID technology include merchandise inventory control, airline luggage location, electronic tolling systems, and human and animal implants.

[8] There are two different aspects of human tracking technology connected with the cellular marketplace. Following issuance of E-911 rules by the Federal Communications Commission in 1997, many cellular companies installed GPS chips in their cell phones. In addition, the location of a powered cell phone can be tracked in real time through the constant and automatic communication between the cell phone and cell towers. *See* Jonathan Krim, *FBI Dealt Setback on Cellular Surveillance*, WASH. POST, Oct. 28, 2005, at A5; Matt Richtel, *Live Tracking of Mobile Phones Prompts Court Fights On Privacy*, N.Y. TIMES, Dec. 10, 2005, at A1.

[9] Biometrics refers to computer-based technology that can identify an individual or verify an individual's identity based on unique physical characteristics known as biometric identifiers including fingerprint imaging, hand and facial geometries, voice recognition, and iris recognition. *See* Eric Lipton, *Hurdles for Technology In U.S. Security Efforts*, N.Y. TIMES, Aug. 10, 2005, at A14; Peter A. Buxbaum, *The Biometrics Dilemma*, HOMELAND SEC., Jan./Feb., 2005, at 14;

Paul Rosenzweig, Alane Kochems & Ari Schwartz, *Biometric Technologies: Security, Legal, and Policy Implications*, THE HERITAGE FOUND., June 21, 2004, www.heritage.org/research/homelanddefense/lm12.cfm.

[10] Human implants frequently contain RFID or GPS technology. The RFID implant is approximately the size of a grain of sand and can be placed under the skin of an arm or a hand utilizing a syringe. In 2004, the United States Food and Drug Administration approved the marketing of RFID microchips. Barnaby J. Feder & Tom Zeller, Jr., *Identity Badge Worn*

autonomy are greatest when GPS, RFID, cellular technology, and biometrics are utilized by the government to conduct surveillance, employers to monitor employees, school districts to track their students, rental car companies to monitor the use of rented vehicles, and parents to keep track of their elusive teenagers.

Currently, the contours of protected privacy remain closely linked to property rights. As will be seen, constitutional protections against technological invasions into privacy remain strongest inside one's home or apartment with the windows shuttered. Once an individual leaves his or her home or is visible inside the home from public space, there is a precipitous drop in the scope of legal protections.

In contrast, many of us still retain a subjective sense of spatial autonomy, even within the eyeshot of the public eye. The concept that one can get lost in a crowd and retain a protected zone of privacy and autonomy currently lacks strong legal foundation. Historically, escape to urban areas constituted a means of obtaining anonymity and a new identity.[11] The growing availability of human tracking technology has the probability of eviscerating any subjective sense of personal autonomy while outside the home unless there is corrective legislative action.

In addition, privacy and other public policy concerns stem from the potential vulnerability of such technologies to hacking and third-party access. A major source of opposition to the United States State Department's plan to introduce an electronic passport program utilizing RFID technology came from those concerned about hacking and surreptitious third-party reading of the information contained in the microchip.[12] At the Fourth Annual IEEE International Conference on Pervasive Computing and Communications in Pisa, Italy in 2006, a computer science research group from Vrije Universiteit in Amsterdam presented a paper identifying potential scenarios involving the vulnerability of RFID tags to worms and viruses.[13] Other computer

---

Under Skin Approved for Use In Health Care, N.Y. TIMES, Oct. 14, 2004 *available at* http://www.nytimes.com/2004/10/14/technology/14implant.html?ei=5070&en=aea96eac9d8c161b&ex=1148529600&adxnnl=1&adxnnlx=1148425670-YYyCA2+3RCqgnWPBR6be3g.

[11] JOHN HOPE FRANKLIN & LOREN SCHWENINGER, RUNAWAY SLAVES: REBELS ON THE PLANTATION 124-148 (1999).

[12] Electronic Passport, 70 Fed. Reg. 61,553-01 (Oct. 25, 2005) (to be codified at 22 C.F.R. pt. 51).

[13] Melanie R. Rieback, Bruno Crispo & Andrew S. Tanenbaum, *Is Your Cat Infected with a Computer Virus?*, http://www.rfidvirus.org/papers/percom.06.pdf; John Markoff, *Study Says Chips in ID Tags Are Vulnerable to Viruses*, N.Y. TIMES, Mar. 15, 2006, at C3.

researchers have demonstrated an ability to hack and clone RFID information.[14] Nevertheless, countries such as China and the United Kingdom are introducing national identification cards containing RFID technology.[15]

Important legal and policy issues also arise in the context of individual volitional use of tracking technology for safety and convenience. The utilization of new technological gadgets can result in unwanted or unanticipated third party surveillance and unforeseen negative consequences such as stalking. Although many motorists enjoy the efficiency of electronic tollbooths and "smart highways," such enjoyment may abruptly end if, or when the government begins to issue speeding tickets premised on the electronic information that calculates the average speed of a trip between two electronic points.[16] The federal government is currently funding state studies regarding the use of GPS tracking on toll roads to develop "mileage-based road user fees."[17] In addition, the popularity of mass transit fare cards with RFID chips may decline when passengers learn that their location and movements can be tracked.[18]

GPS and cellular technology are being utilized for the care of Alzheimer's patients and to enable parents to monitor the location of

---

[14] Robert Lemos, *RFID tags become hacker target*, CNET NEWS.COM, July 28, 2004, http://news.com.com/RFID+tags+become+hacker+target/2100-1029_3-5287912.html.

[15] Sumner Lemon, *China to issue 1.3 billion RFID identification cards*, IDG NEWS SERV., Mar. 9, 2006, http://www.infoworld.com/article/06/03/09/76259_HNchinarfidcards_1.html; Oliver King, *New ID cards defeat for government*, GUARDIAN, Mar. 6, 2006, http://politics.guardian.co.uk/print/0,,329427960-110247,00.html.

[16] Christopher Caldwell, *A Pass On Privacy?*, N.Y. TIMES MAG., July 17, 2005, at 13-14, *available at* http://www.nytimes.com/2005/07/17/magazine/17WWLN.html?ex=1279252800&en=6aa0d44b263846f1&ei=5088&partner=rssnyt&emc=rss.

[17] Declan McCullagh, *Perspective: E-tracking, Coming to a DMV Near You*, CNET NEWS.COM, Dec. 5, 2005, http://news.com.com/E-tracking%2C+coming+to+a+DMV+near+you/2010-1071_3-5980979.html. In New York, over 200 volunteer drivers participated in a federally funded study utilizing GPS devices to create a data flow regarding traffic patterns and speeds in a 40-mile radius. Michael Hill, *Traffic Studied Using Computer-Linked Cars*, ABC NEWS, Apr. 24, 2005, http://abcnews.go.com/US/print?id=698667.

[18] *Oyster Data Uses Rises in Crime Clampdown*, GUARDIAN, Mar. 13, 2006, *available at* http://politics.guardian.co.uk/foi/story/0,,1730771,00.html.

their children.[19] The decreasing expense of GPS devices may tempt some to use tracking technology as a replacement for more expensive nursing and childcare.[20] However, market location devices and services do not constitute "magic bullets" that eliminate fears regarding the safety and well-being of children and the disabled. Satellite-based information regarding the precise location of a patient or child is a far less effective means of protection than direct care. Furthermore, equipment failure or malfunction in such devices and services can increase anxiety, if not panic, for those who choose tracking technology over direct supervision and may result in increased societal costs connected with police intervention.[21]

The legal implications relating to an individual's volitional use of a tracking device to monitor his or her own whereabouts or for safety while driving, hiking, or boating will not be the subject of this article. Reasonable people can differ whether individual use of such technological devices lead to personal serenity or are necessitated by genuine risks to personal safety.[22] There are few justifications for expansive regulation of an individual's choice to utilize new technological gadgets unless the technology results in unwanted or unanticipated third party surveillance, leads to an increase in reckless and anti-social behavior, or is used to intrude on the privacy of others.

Tracking devices, like other technological developments, can lead to unforeseen negative social consequences.[23] On the most basic level,

---

[19] University of Pittsburgh Medical Center, *GPS Technology and Alzheimer's Disease: Novel Use for an Existing Technology*, U. PITT. MED. CENTER, http://alzheimers.upmc.com/GPS.htm (last visited May 13, 2006).

[20] Rob Pegoraro, *Watch Out, Kids: With GPS Phones, Big Mother Is Watching*, WASH. POST, Apr. 19, 2006, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/04/18/AR2006041801604.html.

[21] Matt Richtel, *Selling Surveillance To Anxious Parents*, N.Y. TIMES, May 3, 2006, *available at* http://tech2.nytimes.com/mem/technology/techreview.html?res=9501EED8113FF930A35756C0A9609C8B63.

[22]For example, author Ted Conover has noted that use of a vehicle GPS device can deprive enjoyment "of unmeasured moments of suspension between here and there." Ted Conover, *Get Lost*, N.Y. TIMES, Dec. 14, 2005, *available at* http://www.nytimes.com/2005/12/14/opinion/14conover.html?ex=1292216400&en=6d01289e3e9a5566&ei=5088&partner=rssnyt&emc=rss.

[23] The great television comic Sid Caesar has observed that the use of television remote control devices has led to negative social consequences: "The remote control took over the timing of the world. That's why you have road rage. You have people who have no patience, because you get immediate gratification. You got click, click, click, click. If it doesn't explode within

the expectation of presumed technological perfection in tracking technology can lead to potential panic in the face of a malfunction, anxiety when feeling lost along with a general societal decline in geographical common sense. Although automobile travel has existed for a century, it is only in recent times that some drivers have developed a sense of fear when driving without the availability of a cell phone or outside the range of a cellular tower. Tracking devices can lead to the proliferation of dangerous activities such as reckless mountain hiking to remote areas or over-exuberant geo-caching resulting in police intervention. Nevertheless, a New York Times practical traveler article highlighting the recreational usages of GPS technology failed, to discuss the possibility of mechanical failure or suggest precautions to avoid unexpected exigencies.[24]

The unforeseen societal impact connected with an expansive use of location technology is neither theoretical nor speculative. In an anthropological study of the Inuit people, Professors Claudio Aporta and Eric Higgs analyzed the impact GPS technology has had on the Inuit traditional orientation and navigational skills in the Arctic environment.[25] Historically, the Intuit were able to orient themselves in the harsh Arctic climate through careful observance of natural phenomena such as wind, snowdrifts, and water currents.[26] In their article, Professors Aporta and Higgs describe both the positive and negative consequences from the use of GPS technology by the Inuit. Although hunting for walrus may have become less burdensome, over-reliance on technology has led to a disengagement with the natural world along with hunting mishaps resulting from mechanical failures.[27]

Rapid changes in social behavior and cultural norms caused by the introduction of advanced technologies place a constant pressure for revisions in the legal balance between human rights and property

---

three seconds, click click, click." Hal Boedeker, *PBS' Pioneers' is a history lesson*, CHI. TRIB., Aug. 8, 2005, at 7.

[24] David A. Kelly, *Global Positioning Systems: On Road or Trail, Navigating Made Simple*, N.Y. TIMES, Mar. 5, 2006, *available at* http://travel2.nytimes.com/2006/03/05/travel/05prac.html?pagewanted=1.

[25] Claudio Aporta & Eric Higgs, *Satellite Culture: Global Positioning Systems, Inuit Wayfinding, and the Need for a New Account of Technology*, 46 CURRENT ANTHROPOLOGY 729 (2005).

[26] *Id.* at 731.

[27] *Id.* at 744-745.

rights. A primary area of law that will be subjected to extensive efforts aimed at expanding the zone of protected privacy in the face of human tracking technologies will be provisions of the United States Constitution and analogous provisions of state constitutions. This article begins with a discussion of case law regarding human tracking under the Fourth and Thirteenth Amendments to the United States Constitution and state constitutional provisions.

I. CONSTITUTIONAL LIMITATIONS ON THE USE OF HUMAN TRACKING TECHNOLOGY

The primary source for current American legal analysis of protected privacy interests stems from the field of constitutionally mandated criminal procedure based on judicial interpretations of the Fourth Amendment to the United States Constitution.[28] At present, the United States Supreme Court has not ruled on the applicability of the Fourth Amendment to most recent forms of human tracking technology. Based on precedent over the past four decades regarding the scope of privacy protections under the Fourth Amendment, any expectation for broad judicially based limitations on human tracking technology would be illusory.

The tendency of certain justices and judges to apply judicial restraint with respect to constitutional criminal procedure should not be confused with indifference to the impact technology is having on privacy. Five years ago, Chief Justice Rehnquist, joined by Justices Scalia and Thomas, expressed deep concerns regarding the decline in privacy in the modern technological world:

> Technology now permits millions of important and confidential conversations to occur through a vast system of electronic networks. These advances, however, raise significant privacy concerns. We are placed in the uncomfortable position of not knowing who might have access to our personal and business e-mails, our medical and

[28] The Fourth Amendment provides that: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV.

> financial records, or our cordless and cellular telephone conversations.[29]

Despite such pronouncements, it is unlikely that workable limitations on the use of human tracking devices will grow out of criminal appeals under the Fourth Amendment. In addition, it is unlikely that in the present political climate Congress will increase federal restrictions on tracking technology based on contemporary deregulation ideology and the politics of fear. It is far more probable that broader restrictions will come from state legislative initiatives and judicial interpretations of state constitutional provisions, statutes, and common law.

A. HUMAN TRACKING AND THE FOURTH AMENDMENT

In 1928, fifty years following the invention of the telephone by Alexander Graham Bell, in *Olmstead v. United States*, the United States Supreme Court determined that the Fourth Amendment did not prohibit federal prohibition officials from eavesdropping on telephone conversations taking place in the defendants' homes and offices by inserting small wires on eight telephone lines outside those premises.[30] The *Olmstead* majority reasoned that because the federal agents had placed the wiretaps on the outside they had not engaged in a search or seizure under the Fourth Amendment requiring the issuance of a warrant: "The intervening wires are not part of his house or office any more than are the highways along which they are stretched."[31] Therefore, the majority affirmed the conspiracy convictions under the National Prohibition Act, that were based on the eavesdropping evidence.[32]

Today, the case of *Olmstead v. United States* is primarily remembered for the vigorous dissent authored by Justice Louis D. Brandeis. Well before *Olmstead*, Brandeis was known for his co-authorship of the seminal 1890 Harvard Law Review article "The Right to Privacy," that advocated for enforceable common law rights

---

[29] Bartnicki v. Vopper, 532 U.S. 514, 541 (2001) (Rehnquist, C.J., dissenting). In that same year, Justice Scalia observed that "[i]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology." Kyllo v. United States, 533 U.S. 27, 33-34 (2001).

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

[30] *Id.* at 465.

[32] *Id.* at 469.

against the invasion of personal privacy, especially in the face of the development of new technologies such as photography.[33]

In his *Olmstead* dissent, Brandeis presented a far-sighted critique regarding the government's use of the new technology to invade the privacy of its citizens. In contrast to the majority's reliance on concepts of trespass law to limit the zone of privacy protected by the Fourth Amendment, Brandeis articulated a broader concept of constitutionally protected privacy that transcends both property interests and materialism:

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone-- the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.[34]

Close to forty years later, the United States Supreme Court overruled the holding in *Olmstead v. United States*. In *Katz v. United States*, the Court held that the FBI's placement of a microphone on the roof of an enclosed public telephone booth to eavesdrop and tape record telephone calls made by an illegal gambling suspect, without a warrant, constituted a violation of the Fourth Amendment regardless of whether or not a physical intrusion had taken place.[35] In reaching its decision in *Katz*, the Court's majority rejected both a strict reliance on trespass law to define the scope of privacy protections under the Fourth Amendment, as well as Brandeis' much broader concept that

---

[33] Samuel L. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890); *See also* David W. Leebron, *The Right to Privacy's Place in the Intellectual History of Tort Law*, 41 CASE W. RES. L. REV. 769 (1991); JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 5-7 (2000) [hereinafter UNWANTED GAZE].

[34] *Olmstead*, 277 U.S. at 478 (Brandeis, J., dissenting).

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

the Fourth Amendment gave Americans "the right to be let alone" by other people.[36] Nevertheless, by mandating for the first time that the police obtain a court-ordered warrant before engaging in electronic surveillance, the *Katz* decision established a significant judicial check on government agents randomly engaging in such surveillance.[37]

In his concurrence in *Katz*, Justice Harlan formulated the now uniform test for determining whether the Fourth Amendment is applicable to a particular set of facts, including whether a particular use of a new invasive technology is unconstitutional: a) whether the individual possesses a subjective expectation of privacy, and b) whether the individual's subjective expectation is "one that society is prepared to recognize as 'reasonable.'"[38] Despite continued judicial reliance on Justice Harlan's *Katz* formulation regarding the applicable test for what constitutes a protected expectation of privacy, as early as 1971, Justice Harlan distanced himself from the formulation, noting that it can "lead to the substitution of words for analysis" and emphasized that the critical question "is whether under our system of government, as reflected in the Constitution, we should impose on our citizens the risks of the electronic listener or observer without at least the protection of a warrant requirement."[39]

B. THE FOURTH AMENDMENT OUTSIDE AND INSIDE THE HOME

The *Katz* reasonable expectation of privacy test has led to a series of federal court decisions that have determined that, in most cases, the use of a tracking device to monitor the location of vehicles and containers are not subject to the Fourth Amendment. The primary exception to this rule is when the device is utilized to determine what is taking place within a person's home.

In 1983, in *United States v. Knotts*, the Supreme Court decided that the police did not have to obtain a warrant under the Fourth Amendment before using a radio beeper to monitor the movement and location of a vehicle.[40] The Court portrayed the use of such tracking

---

[36] *Id.* at 350 (stating that "the correct solution of Fourth Amendment problems is not necessarily promoted by incantation of the phrase "constitutionally protected area." Secondly, the Fourth Amendment cannot be translated into a general constitutional "right to privacy").

[37] *Id.* at 350-353.

[38] *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

[39] United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting).

[40] United States v. Knotts, 460 U.S. 276 (1983).

technology as a mere extension of the police's power to engage in visual surveillance of a criminal suspect.[41]

In *Knotts*, the police had placed a battery operated radio transmitter in a drum containing chloroform as part of a drug investigation.[42] After the drug suspect purchased the drum, the police used the beeper's signals to assist in conducting surveillance of the movement and location of the suspect's car containing the drum of chloroform.[43] The beeper transmissions, along with additional visual surveillance by the police, resulted in the issuance of a warrant and the disclosure of a clandestine drug laboratory located in a rural Wisconsin cabin.[44] In reaching its decision, the Supreme Court applied a broad legal rule that renders the use of most human tracking devices attached to vehicles to be outside of Fourth Amendment protections: "A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[45]

Under *Knotts*, whether the vehicle is driven unseen on an empty highway, through a long dark tunnel, or an unpaved obscure mountainous road, is irrelevant. The mere exposure of the vehicle to the sunlight or the exterior darkness grants the police, without a warrant, to monitor the movement of the vehicle utilizing a tracking device lawfully placed.

The principle applied in *Knotts* was based on earlier cases that had determined that Americans, in general, have few Fourth Amendment privacy rights while outside the home. This exception to Fourth Amendment protections has been long recognized by the Supreme Court. For example, in *Hester v. United States*, the Court determined that Fourth Amendment protections did not extend from a house into an adjacent open field.[46] Sixty years later, the open fields exception to the Fourth Amendment was reaffirmed in *Oliver v. United States*.[47]

---

[41] *Id.* at 280-282.

[42] *Id.* at 277.

[43] *Id.*

[44] *Id.*

[45] *Id.* at 281.

[46] Hester v. United States, 265 U.S. 57 (1924).

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

Intentional or inadvertent exposure can also defeat a claimed expectation of privacy. Therefore, the Fourth Amendment has been found inapplicable to aerial police observation of an area from public air space.[48] Similarly, the Court has held that the Fourth Amendment was not violated when law enforcement stood in an open field and observed the inside of a barn that was 60 yards from a home.[49]

It is reasonable to assume that this limited conception of privacy under the Fourth Amendment would be equally applicable to the use of location devices that are legally attached or carried by an individual on public streets, roads, and trails. An expansive application of this principle to new location technology in an unregulated market economy would permit anyone to electronically track anyone else in public.

One year after *Knotts*, the Supreme Court in *United States v. Karo* was called upon to determine whether the police violated the Fourth Amendment when they attached a beeper to a can of chemicals during another drug investigation to determine the can's location within a private residence not open to visual surveillance.[50] Like *Knotts*, the police in *Karo* had used beeper transmissions and visual surveillance to follow the movement of the can to various locations.[51] However, unlike *Knotts*, the police continued to utilize the beeper to determine whether the can was located in the private house.[52] In concluding that the Fourth Amendment had been violated, the *Karo* majority applied a core Fourth Amendment principle that a search and seizure inside a home without a warrant is presumptively unreasonable absent an exigent circumstance.[53] Based on the fact that the beeper allowed the police to learn that the can was located in the house and allowed for them to monitor its internal movement, the Court concluded that the use of the tracking device constituted an unlawful search under the Fourth Amendment.[54]

---

[48] California v. Ciraolo, 476 U.S. 207 (1986).

[49] United States v. Dunn, 480 U.S. 294 (1987).

[50] United States v. Karo, 468 U.S. 705, 707 (1984).

[51] *Id.* at 708.

[52] *Id.*

[53] *Id.* at 714.

[54] *Id.* at 714-715.

The broad scope of judicially recognized Fourth Amendment protections against technological surveillance within the home was exemplified in the 2001 decision in *Kyllo v. United States*.[55] At the same time, the *Kyllo* decision suggests that the proliferation of invasive technological tools in general public use may eviscerate any reasonable expectation to privacy within one's home.

In *Kyllo*, the police suspected that marijuana was being grown inside a home utilizing high-density halide lamps.[56] In order to determine whether such lamps were being utilized, the police while seated in their car in the street, scanned the home utilizing a thermal imager to detect infrared radiation that is invisible to the naked eye.[57] The scanning device reported that portions of the house were hotter than other sections of the house and neighboring homes.[58] In concluding that the police's use of the thermal-imaging device without a warrant violated the Fourth Amendment because it was capable of detecting lawful behavior in the house, the *Kyllo* majority stated:

> Where, as here, 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.[59]

At present, the Supreme Court has not interpreted the Fourth Amendment with regard to more advanced forms of tracking technology such as GPS, RFID, or real time cell site monitoring. Based on Supreme Court precedent since *Katz*, it is unlikely that the Court will rule that the Fourth Amendment requires a warrant prior to the police utilizing such devices to electronically track movement in public. However, a strong argument can be made that based on the scope of private information obtainable through GPS and cellular tracking technology, the Fourth Amendment probable cause and

---

[55] Kyllo v. United States, 533 U.S. 27 (2001).

[56] *Id.* at 29.

[57] *Id.*

[58] *Id.* at 30.

[59] *Id.* at 40.

warrant requirements should be found applicable.[60] In 2005, a Federal District Court in New York, relying on the *Knotts* decision, ruled that the Fourth Amendment was not violated when the police attached GPS devices to the defendant's vehicles because the defendant had no expectation of privacy while driving on public roadways.[61] In contrast, a federal judge in Maryland has questioned, without deciding, whether the extraordinary amount of detailed personal information obtainable through the use of a GPS device would render it subject to Fourth Amendment constraints.[62]

The *Kyllo* and *Karo* decisions strongly suggest that the use of GPS, RFID, and real time cell site technology by the police to monitor the location of an individual or object within a home will be subject to the requirements of the Fourth Amendment. Based on the portability of cell phones, lawful public location surveillance by the police under *Knotts* can easily be transformed into unlawful surveillance under *Karo* if the cell phone is being carried into a home or other private space. Last year, three United States District Court Magistrates issued decisions raising such Fourth Amendment concerns with respect to warrantless real time cell site monitoring.[63]

Finally, it should not be overlooked that the *Kyllo* decision contains an ominous caveat regarding Fourth Amendment protections against electronic surveillance within a home: it is limited to devices that are not "in general public use."[64] This expressed limitation in the *Kyllo* holding raises the possibility that the proliferation of cell phones and inexpensive GPS devices could lead the Supreme Court to conclude that electronic monitoring within a home using such devices is not subject to the Fourth Amendment.

---

[60] The Washington Supreme Court adopted this reasoning when it interpreted that State's broader constitutional provision protecting "private affairs." State v. Jackson, 76 P.3d 217 (Wash. 2003) (en banc); *see also* Otterberg, *supra* note 6, at 695-697.

[61] United States v. Moran, 349 F. Supp 2d 425, 467-468 (N.D.N.Y. 2005).

[62] United States v. Berry, 300 F. Supp 2d 366, 368 (D. Md. 2004).

[63] *See In re* Application for Pen Register and Trap/Trace Device with Cell Site Location Authority, 396 F. Supp 2d 747 (S.D. Tex. 2005)*; In the Matter of an* Application of the United States for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device and (2) Authorizing Release of Subscriber Information and/or Cell Site Information, 396 F. Supp 2d 294 (E.D.N.Y. 2005); *In re* Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register and a Caller Identification System on Telephone Numbers [Sealed] and [sealed] the Production of Real Time Cell Site Information, 402 F. Supp 3d 597 (D. Md. 2005).

[64] *Kyllo*, 533 U.S. at 40.

C. THE THIRTEENTH AMENDMENT AND HUMAN TRACKING

Professors Jerome Dobson and Peter F. Fisher have applied the term "geoslavery" to describe how new location tracking devices can result in coercive control over human movement and direction.[65] The metaphorical application of the term "slavery" to electronic human tracking has both historical precedence and legal relevance.[66] From well before the Civil War through the 1930s, phrases such as "wage slavery" and "industrial slavery" were frequently applied to describe the oppressed conditions and status of workers.[67] The brutal reality of chattel slavery was obviously and substantially more oppressive than 19th Century working conditions or contemporary use of electronic monitoring. Nevertheless, in considering possible legal restraints applicable to human tracking it is relevant to consider the value such devices would have had for slaveholders in the 19th Century, the impact such technology would have had on American history, and whether such devices constitute a vestige of slavery.

Historians John Hope Franklin and Loren Schweninger have detailed and documented the amount of time and resources Southern slaveholders had to expend in searching for and capturing runaway slaves.[68] Their study highlights that essential aspects of American slavery included restrictions on the freedom of movement of enslaved African-Americans and severe corporal punishment imposed by slaveholders and overseers when slaves were caught escaping or captured following escape.

Many in bondage attempted and succeeded in escaping for different motives including legal emancipation, reunions with family members, and escape from particularly brutal owners. The method and direction of escape differed widely, causing slave owners to rely on speculation and surmise in tracking down their escaped human property.[69] As a means of locating and capturing those who escaped, slaveholders hired lawyers, petitioned state legislatures, purchased newspaper advertisements, and utilized slave catchers. These means of human tracking were expensive and inefficient.

---

[65] Jerome E. Dobson & Peter F. Fisher, *Geoslavery*, IEEE TECH. AND SOC'Y MAG., Spring 2003, at 47.

[66] *See* FONER, *supra* note 1, at 29-31.

[67] *Id.* at 60-62, 142, 199-203.

[68] FRANKLIN & SCHWENINGER, *supra* note 11, at 149-181.

[69] *Id*. at 97-123.

American concerns regarding the location and capture of those who escaped from bondage can be found in the United States Constitution. Slaveholder interest in maintaining physical and legal control over their human chattel was so great that the Constitution was drafted to contain the Fugitive Slave Clause aimed at guaranteeing the return of a runaway who succeeded in an interstate escape.[70] The Fugitive Slave Clause, originally proposed by a South Carolina delegate to the Constitutional Convention, was aimed at insuring that slaveholders had a constitutionally based means of obtaining the return of a runaway slave who had escaped to a free state without the drafters' using the word slavery.[71] In 1793, the Second Congress enacted legislation granting slaveholders and their agents a specific legal procedure permitting them to seize an individual and take him or her before a magistrate to obtain a certificate requiring a return to bondage in a slave state.[72]

As part of the Compromise of 1850, Congress enacted the Fugitive Slave Act aimed at easing the ability of Southern slaveholders to recapture fugitive slaves through Federal judicial means. However, rather than calming the rising national dispute over slavery, the provisions of the Fugitive Slave Act precipitated an increase in aggressive Abolitionist activity including active resistance to the capture of freed slaves.[73]

The 1851 *Thomas Sims's Case* is an example of the type of antebellum litigation that resulted when slave owners sought the return of a runaway.[74] On April 3, 1851, under the powers of the Fugitive Slave Act of 1850, Commissioner George T. Curtis of the United States Circuit Court issued a warrant to the Massachusetts federal marshal requiring the capture of Sims, an African-American "fugitive

---

[70] The United States Constitution states, "No Person held to Service or Labour in one State, under the Laws thereof, escaping into another, shall, in Consequence of any Law or Regulation therein, be discharged from such Service or Labour, but shall be delivered up on Claim of the Party to who such Service or Labour may be due." U.S. CONST. art. IV, § 2, cl. 3.

[71] JACK N. RAKOVE, ORIGINAL MEANINGS: POLITICS AND IDEAS IN THE MAKING OF THE CONSTITUTION 89, 91 (1996).

[72] Thomas Sims's Case, 61 Mass. (1 Cush.) 285, 297-298, 301-302 (1851).

[73] RICHARD H. SEWELL, BALLOTS FOR FREEDOM: ANTISLAVERY POLITICS IN THE UNITED STATES 1837-1860 236-239 (1976); HENRY MAYER, ALL ON FIRE: WILLIAM LLOYD GARRISON AND THE ABOLITION OF SLAVERY 406-442 (1998); MILTON C. SERNETT, NORTH STAR COUNTRY: UPSTATE NEW YORK AND THE CRUSADE FOR AFRICAN AMERICAN FREEDOM 127-153 (2002).

[74] Thomas Sims's Case, 61 Mass. (1 Cush.) 285 (1851).

from labor" to answer a complaint filed on behalf of a Georgia slave owner.[75] Following Sims's capture and imprisonment pursuant to the warrant, a habeas corpus petition was filed in Massachusetts's state court seeking to free Sims and challenging the Fugitive Slave Law. The petition was heard before Massachusetts' Chief Judge Lemuel Shaw, the father-in-law of Herman Melville. To avoid the recurrence of Abolitionists' physical efforts to rescue Sims, heavy chains were placed around the courthouse.[76] Although personally opposed to slavery, Chief Judge Shaw denied the writ concluding that the Fugitive Slave Act was constitutional based on the history of the Fugitive Slave Clause and precedent upholding the earlier 1793 federal fugitive slave law.[77] Following Chief Judge Shaw's application of judicial restraint, Sims was returned to bondage in Georgia and subjected to a severe public beating.[78]

The use of GPS, RFID, and biometric technology by slave owners would have perpetuated the enslavement of African-Americans, substantially decreased the cost of tracking down runaways, and altered American history. The use of real time location technology would have vastly improved the monitoring of the daily productivity of slave labor, thereby increasing efficiency along with the economic value and power of America's peculiar institution. Such technology would have also made slave resistance and escape far more difficult. Through GPS or RFID implants, slaveholders would have been able to easily locate and identify individuals who succeeded in escaping. Working together, slaveholders would have been able to establish geo-fences and a communications network that would have substantially aided in slaveholder domination over the personal lives of those held in bondage. By undermining the ability of individuals such as Frederick Douglass from escaping, these technological tools may have decreased the awareness in the North of the horrors of American slavery prior to the Civil War.[79]

In 1865, Congress adopted the Thirteenth Amendment, subsequently ratified by the States, banning slavery and involuntary servitude. Unlike other constitutional amendments, the Thirteenth

---

[75] *Id.* at 293.

[76] ANDREW DELBANCO, MELVILLE: HIS WORLD AND WORK 153-154 (2005).

[77] *Sims*, 61 Mass. (1 Cush). at 294-308.

[78] DELBANCO, *supra* note 76, at 154.

[79] *See* WILLIAM S. MCFEELY, FREDERICK DOUGLASS (1991).

Amendment uniquely restricts both private conduct as well as governmental action.[80] The Thirteenth Amendment states:

> 1. Neither slavery nor involuntary servitude, except as a punishment for crime whereof the party shall have been duly convicted, shall exist within the United States, or any place subject to their jurisdiction.
>
> 2. Congress shall have power to enforce this article by appropriate legislation.[81]

The Thirteenth Amendment was never intended to be limited to ending the enslavement of African-Americans. In 1911, the United States Supreme Court highlighted the amendment's broad breadth when it described the amendment as "a charter of universal civil freedom for all persons, of whatever race, color or estate, under the flag" that was intended to abolish both slavery as well as all vestiges, badges, and incidents of slavery.[82] In addition to outlawing slavery, the Thirteenth Amendment also prohibits involuntary servitude.

The amendment granted Congress the power to enact legislation targeted at eliminating those badges and incidents of slavery including the "privilege to go and come" as one pleases.[83] Congressional authority under the amendment includes the power "to determine what are the badges and the incidents of slavery, and the authority to translate that determination into effective legislation."[84] However, it was not intended to be the basis for challenging various established societal power relationships such as that of parent-child.[85]

Based on the history and interpretation of the Thirteenth Amendment, Alexander Tsesis has argued that the amendment

---

[80] United States v. Kozminski, 487 U.S. 931, 942 (1988).

[81] U.S. CONST. amend XIII.

[82] Bailey v. State of Alabama, 219 U.S. 219, 241 (1911).

[83] Jones v. Alfred H. Mayer Co, 392 U.S. 409, 430 (1968) (quoting from Senate Judiciary Chairman Trumbell during a 1866 legislative debate).

[84] *Id.* at 440.

[85] *Kozminski*, 487 U.S. at 944 (citing Robertson v. Baldwin, 165 U.S. 275, 282 (1897)).

provides the constitutional predicate for the enactment of broad federal laws banning public and private limitations on universal liberties.[86]

Whether a majority of the United States Supreme Court would concur with Tsesis' thesis of such broad congressional power under the Thirteenth Amendment remains in doubt. Various Supreme Court decisions in the past fifteen years have demarcated newly established limitations on congressional legislative power under the Commerce Clause, the Eleventh Amendment, and the remedial provision of the Fourteenth Amendment.[87]

Nevertheless, a reasonably strong argument can be made that Congress does have the constitutional power under the remedial provision of the Thirteenth Amendment to ban the use of tracking devices to dominate and control the location of others. Imposing restrictions, control, and monitoring over another's location constitutes a vestige and incident of slavery.

In addition, mandatory tracking, identification implants, or attachments on another human being would be subject to court challenge under the Thirteenth Amendment. Such devices are the technological equivalent, in many respects, to various slaveholder tools, including branding, utilized to keep African-Americans from escaping bondage or as punishment for such escapes. Therefore, the use of such devices to establish geo-fences and even impose corporal punishment would constitute a vestige of slavery. In addition, the imposition of physical injury or threat of physical injury emanating from a tracking device would be subject to challenge as a form of involuntary servitude especially if the electronic punishment is aimed at forcing an individual to continue working.[88]

---

[86] ALEXANDER TSESIS, THE THIRTEENTH AMENDMENT AND AMERICAN FREEDOM: A LEGAL HISTORY 86-87, 89, 104-105 (2004).

[87] *See* United States v. Lopez, 514 U.S. 549 (1995) (in which a Federal statute prohibiting guns in the vicinity of public schools was declared unconstitutional on the grounds that it went beyond congressional power granted by the Commerce Clause); Alden v. Maine, 527 U.S. 706 (1999) (in which a Federal overtime law was determined to be unconstitutional under the Eleventh Amendment to the extent that it granted employees the right to sue State employers in Federal court); United States v. Morrison, 529 U.S. 598 (2000) (in which a portion of the Federal Violence Against Women Act was declared unconstitutional as beyond congressional authority under the Commerce Clause and the Fourteenth Amendment); Board of Trustees of University of Alabama v. Garrett, 531 U.S. 356 (2001) (holding the Americans with Disabilities Act unconstitutional under the Eleventh Amendment to the extent that it applied to a State's workforce).

[88] Dobson & Fisher, *supra* note 64, at 47-49; Peter Fisher & Jerome Dobson, *Who Knows Where You Are, and Who Should, in the Era of Mobile Geography?* 88 GEOGRAPHY 331, 335-336 (2003); *Kozminski*, 487 U.S. at 944, 952.

D. STATE CONSTITUTIONAL LIMITATIONS ON THE USE OF TRACKING DEVICES

The application of the reasonable expectation of privacy test to new technological intrusions is not without its critics. As Jeffrey Rosen has pointed out, "[A]s advances in the technology of monitoring and searching have made ever more intrusive surveillance possible, expectations of privacy have naturally diminished, with a corresponding reduction in constitutional protections."[89] The Oregon Supreme Court in *State v. Campbell* termed the reasonable expectation test as "a formula for expressing a conclusion rather than a starting point for analysis, masking the various substantive considerations that are the real bases on which Fourth Amendment searches are defined."[90]

Various state courts have determined, under their respective state constitutions, that the police are required to obtain a warrant prior to utilizing an electronic device. In reaching such legal conclusions, the courts have recognized that electronic tracking devices are not mere technological enhancements to law enforcement vision but rather a substantial intrusion into an individual's privacy and autonomy.

In *State v. Campbell*, the Oregon Constitution was interpreted to prohibit the police's warrantless use of a radio transmitter to locate a private vehicle.[91] In that case, the police used a radio transmitter attached to a burglary suspect's car to track his movements after the police were unable to maintain constant visual surveillance.[92] In determining that a warrant is required prior to the police utilizing a tracking device, the Oregon Supreme Court rejected the Supreme Court's rationale in *Knotts* and determined that the transmitter was a location finder rather than a mere extension of police visual tracking.[93] In substitution of the reasonable expectation of privacy test, the Oregon Supreme Court defined a privacy interest as "an interest in freedom from particular forms of scrutiny" and concluded that the use

---

[89] ROSEN, UNWANTED GAZE, *supra* note 32, at 60-61.

[90] State v. Campbell, 759 P.2d 1040, 1044 (Or. 1988).

[91] *Id.* at 1041.

[92] *Id.*

[93] *Id.* at 1047.

of a radio transmitter to locate a person or object constituted a significant limitation on the freedom from scrutiny.[94]

In reaching its conclusion, the Oregon Court recognized the perniciousness of technological tracking devices by creating a daily fear of being watched:

> The limitation is made more substantial by the fact that the radio transmitter is much more difficult to detect than would-be observers who must rely upon the sense of sight. Without an ongoing, meticulous examination of one's possessions, one can never be sure that one's location is not being monitored by means of a radio transmitter. Thus, individuals must more readily assume that they are the objects of government scrutiny.[95]

In 2003, the Washington Supreme Court ruled that under Washington's more protective constitutional provision regarding searches and seizures, the police were required to obtain a warrant based on probable cause prior to attaching a GPS device to a citizen's vehicle.[96] In accordance with the Oregon Supreme Court's analysis, Washington's highest court concluded that a GPS device replaces rather than augments police visual surveillance. In reaching its decision, Washington's highest court recognized the enormous intrusive power of GPS devices to provide a detailed picture of an individual's daily life, stating that:

---

[94] *Id.* However, more recently in State v. Meredith, 96 P.3d 342 (Or. 2004), the same court found that the police's warrantless use of a beeper on an employer's vehicle, with the employer's consent, did not violate the employee's privacy rights under Oregon's constitution.

[95] *Campbell*, 759 P.2d at 1048. American history over the past century provides a reasonable basis for concerns relating to unlawful electronic surveillance of legitimate political activities. *See* TAYLOR BRANCH, PILLAR OF FIRE: AMERICA IN THE KING YEARS 1963-65 (1998); DAVID J. GARROW, THE FBI AND MARTIN LUTHER KING, JR. (1981). At the same, publicity surrounding the use of electronic tracking devices can lead to irrational concerns. *See* Dunne v. Police Department, 128 F. App'x 673 (9th Cir. 2005) (in which the plaintiff claimed that a GPS device had been implanted in his left eye socket to render him a sex slave. The case was dismissed because he was unable to prove the existence of the GPS implant).

[96] State v. Jackson, 76 P.3d 217 (Wash. 2003) (en banc). Article I, § 7 of the Washington Constitution provides that "[n]o person shall be disturbed in his private affairs, or his home invaded, without authority of law." WASH. CONST. art. I, § 7.

> [U]se of GPS tracking devices is a particularly intrusive method of surveillance, making it possible to acquire an enormous amount of personal information about the citizen under circumstances where the individual is unaware that every single vehicle trip taken and the duration of every single stop may be recorded by the government.[97]

Two New York State trial courts have rendered conflicting decisions regarding whether the New York State Constitution requires the police to obtain a warrant prior to attaching a GPS device to a vehicle. In *People v. Lacey*, one county judge, without articulating a developed legal analysis, concluded in 2004 that a warrant was required.[98] Last year, another county judge reached the opposite conclusion based on the *Knotts* analysis that an individual does not have a legitimate expectation of privacy while driving on public roads.[99]

In addition to state constitutional limitations regarding governmental search and seizure, certain states have explicit constitutional privacy provisions that may form the basis for future challenges to governmental and private use of tracking devices. For example, California Constitution, Art. 1, § 1 contains an explicit reference to a right of privacy applicable to both private as well as state conduct.[100] In 1970, Illinois, in direct response to the development of new intrusive technologies, amended its constitution to include an express provision protecting its citizens against invasions of privacy, including the use of electronic surveillance.[101] Other states

---

[97] *Jackson*, 76 P.3d at 224; *see also* State v. Kelly, 708 P.2d 820 (Haw. 1985) (in which the Hawaii Supreme Court ruled that the police's warrantless installation of a beeper in a photograph album was both an unreasonable search and seizure under the Hawaiian Constitution).

[98] People v. Lacey, Indictment No. 2463N/02, 2004 WL 1040676 (Nassau, N.Y. County Ct. May 6, 2004).

[99] People v. Gant, 9 Misc. 3d 611 (Westchester, N.Y. County Ct. 2005).

[100] The California Constitution states, "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." CAL. CONST. art. 1, § 1.

[101] The Illinois Constitution provides, "The people shall have the right to be secure in their persons, houses, papers and other possessions against unreasonable searches, seizures, invasions of privacy or interceptions of communications by eavesdropping devices or other means. No warrant shall issue without probable cause, supported by affidavit particularly

such as Hawaii, Alaska, and Florida have similar specific state constitutional provisions protecting the right to privacy.[102]

Nevertheless, it remains unclear how these various state constitutional privacy provisions will be applied to new electronic tracking devices. Unlike Oregon's highest court, the California Supreme Court in *Hill v. NCAA*, ruled that in order to be able to allege a violation of California's constitutional right to privacy, a plaintiff must establish a violation of a reasonable expectation of privacy.[103] Under the standards set forth in *Hill v. NCAA*, a reasonable expectation of privacy under the California constitution will be determined by state judges based on a variety of objective considerations, borrowed from the common law, including advanced warning or consent, community customs, norms, and practices and the physical setting of the particular activity.[104] Constitutional privacy challenges in California to a fingerprint requirement for a driver's license and biometric finger-imaging requirement for public assistance have been unsuccessful.[105] It remains to be seen whether the state constitutional right to privacy in California will be interpreted to place limitations on the use of electronic surveillance to track public

---

describing the place to be searched and the persons or things to be seized." ILL. CONST. art. 1, § 6.

[102] The Hawaiian Constitution states, "The right of the people to privacy is recognized and shall not be infringed without the showing of a compelling state interest. The legislature shall take affirmative steps to implement this right." HAW. CONST. art. 1, § 6. Similarly, the Alaskan Constitution states, "The right of the people to privacy is recognized and shall not be infringed. The legislature shall implement this section." ALASKA CONST. art. I, § 22. Likewise, the Florida Constitution states, "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. This section shall not be construed to limit the public's right of access to public records and meetings as provided by law." FLA. CONST. art. 1 § 23.

[103] Hill v. Nat'l Collegiate Athletic Ass'n, 865 P.2d 633, 655 (Cal. 1994); *see also* State v. Glass, 583 P.2d 872, 875 *(*Alaska 1978*)* (in which the Alaska Supreme Court explicitly adopted Justice Harlan's formulation in *Katz* to the Alaska's state constitutional right to privacy, making the law in Alaska similar to that of California in requiring that there be a reasonable expectation of privacy before there can be a violation of the right to privacy).

[104] *Hill*, 865 P.2d at 655.

[105] Perkey v. Department of Motor Vehicles, 228 Cal. Rptr. 169 (1986) (finding that a mandatory fingerprint requirement did not violate the U.S. Constitution, holding that the requirement violated California statutory provisions, and declining to determine whether the requirement violated the California Constitution); Sheyko v. Saenz, 5 Cal. Rptr. 3d 350 (Ct. App. 2003). In addition, constitutional challenges on religious grounds to biometric imaging have been rejected by state appellate courts in California and New York. *Id.;* Medvedev v. Wing, 671 N.Y.S.2d 806 (N.Y. App. Div. 1998).

activities. The extraordinary speed of technological innovation in the field of human tracking has created constantly evolving legal, public policy, and ethical challenges. The recent introduction of human tracking implants into medicine, patient care, employment, and recreation raises substantial questions regarding whether current law provides an appropriate and satisfactory framework to protect individual privacy and liberty.

II. THE LEGAL IMPLICATIONS OF HUMAN TRACKING IMPLANT TECHNOLOGY

The development, marketing, and use of human subdermal RFID and GPS implants raise challenging and new legal and ethical issues. As early as 1985, California veterinarian Hannis L. Stoddard was working on the development of an implantable identification chip for use with animals.[106] Implanted RFID tracking devices are used frequently in the identification of animals. The British company Trovan, Ltd. markets various forms of implantable transponders and readers throughout the world for animal and human identification.[107] GPS and RFID implants are being marketed for the monitoring, control, identification, and return of domestic animals. Through GPS technology, a pet owner can create a virtual fence for the pet and receive email messages regarding its location.[108]

Both Congress and state legislatures have enacted laws embracing the use of RFID implants for domestic and farm animals. On

---

[106] Hannis L. Stoddard, III, *How AVID started*, http://www.avidid.com/stoddard.html (last visited May 17, 2006).

[107] Trovan, *Electronic Identification Systems*, http://www.trovan.com/company.htm (last visited May 17, 2006). One example of the ubiquitous use of Trovan products was observed fortuitously during a 2005 family visit to Namibia where leopards have been implanted with Trovan RFID devices as part of a concerted effort to preserve their endangered population. During the same trip, I observed elephants with GPS devices around their necks as part of a study of their migration patterns in southern Africa.

[108] Anne Eisenberg**,** *For the Fretting Pet Owner, a Wireless Distress Signal*, N.Y. TIMES, July 15, 2004, available at http://www.nytimes.com/2004/07/15/technology/circuits/15next.html?ex=1247630400&en=68121d87ca4dd70d&ei=5090&partner=rssuserland; Kathleen Megan, *GPS designed to find lost pets, notify owners*, MIAMI HERALD, Feb. 12, 2006, available at http://www.miami.com/mld/miamiherald/living/home/pets/13843615.htm. *The Schering-Plough Animal Health Corporation markets the HomeAgain® pet recovery service that utilizes RFID implants.* See *HomeAgain® Pet Recovery Service*, HomeAgain Information Center, http://www.homeagainpets.com/.

November 10, 2005, President George W. Bush signed into the law the Agriculture, Rural Development, Food and Drug Administration, and Related Agencies Appropriations Act, 2006.[109] This Act mandates and funds the establishment of a national RFID animal microchip system, as well as requires the United States Department of Agriculture to promulgate regulations regarding the system.[110]

Various states including Minnesota, Oregon, New York, and Colorado have codified procedures for implanting microchips in dangerous or potentially dangerous dogs.[111]

The first known experiment regarding the use of a human tracking implant took place at the University of Reading in England in 1998.[112] Professor of Cybernetics, Kevin Warwick, had an RFID tracking device implant placed in his arm that enabled him to monitor his movements on campus for one week.[113] An expressed purpose for the experiment was to demonstrate the inherent dangers to personal privacy connected with implant technology.[114]

Dr. John D. Halamka, the Chief Information Officer for the Harvard Medical Center, has conducted a more recent and longer experiment in the use of a voluntary human RFID implant containing a 16-digit medical identifier.[115] With the use of a handheld RFID transponder, Dr. Halamka's implanted identifier can be obtained and used to discover his identity and his doctor through an internet site maintained by the manufacturer.[116] Significantly, the implant does not include any medical history or any known disabilities and is not equipped to monitor Dr. Halamka's location. His willingness to

---

[109] Agriculture, Rural Development, Food and Drug Administration, and Related Agencies Appropriations Act, 2006, Pub. L. No. 109-97, 119 Stat. 2120 (2005).

[110] *Id.*

[111] MINN. STAT. § 347.515 (2006); OR. REV. STAT. § 609.168 (2006); COLO. REV. STAT. § 18-9-204.5(3)(e.5) (2006); N.Y. AGRIC. & MKTS. LAW § 121(2) (Consol. 2006).

[112] *Technology gets under the skin*, BBC NEWS, Apr. 24, 1998, http://news.bbc.co.uk/1/hi/sci/tech/158007.stm.

[113] *Id.*

[114] *Id.*; *See also* The University of Reading, *Professor Kevin Warwick*, http://www.kevinwarwick.org (last visited May 17, 2006).

[115] John Halamka, *Straight from the Shoulder*, 353 NEW ENG. J. MED. 331, 331-332 (2005).

[116] *Id.* at 331.

participate in the experiment was an outgrowth of Dr. Halamka's experiences as an emergency room resident when he was unable to determine the identification of patients.[117] In his article, Dr. Halamka acknowledges the possibility that the implant can lead to invasion of privacy due to the non-use of encryption technology, the unauthorized use of transponders and hacking.[118] In response to claims by others that human implant chips are Orwellian in nature, Dr. Halamka concedes: "I have not investigated these or other moral, religious, or political implications of having an implanted identifier."[119]

The American company, Applied Digital Solutions, Inc., is aggressively marketing its RFID VeriChip™ human implant to hospitals and doctors in the United States for the same emergency room purposes articulated by Dr. Halamka. Last year, a New Jersey hospital was the first to commence the regular scanning of emergency room patients for a medical identification number contained in the microchip.[120] Approximately 80 hospitals and medical centers in the United States have since agreed to utilize the RFID implant system.[121] This hospital based marketing has succeeded in persuading patients to consent to receiving implants.[122] Other hospitals around the country have received RFID scanners and may begin utilizing the technology in their emergency rooms.[123]

In general, the marketing and publicity surrounding these implant products focus on the purported convenience, security, and the ability to alleviate fear. The impact on personal privacy, the products' reliability, and the interception of data by third parties has not received similar coverage. However, the recent scholarly paper describing the potential vulnerability of RFID technology to cyber viruses and worms

---

[117] *Id.*

[118] *Id.* at 332.

[119] *Id.* at 333.

[120] Rob Stein, *Use of Implanted Patient-Data Chips Stirs Debate on Medicine vs. Privacy*, WASH. POST, Mar. 15, 2006, at A1.

[121] Press Release, Verichip Corp., *172 New Physicians Elect to Offer VeriMed ID System to Patients* (Mar. 20, 2006), http://www.verichipcorp.com/news/1142883972.

[122] Halamka, *supra* note 113, at 333; Cristina Odone, *How We'll Keep Tags on the Old Folk*, OBSERVER, Mar. 19, 2006, http://observer.guardian.co.uk/comment/story/0,,1734263,00.html.

[123] Halamka, *supra* note 115, at 333.

may constitute a powerful antidote to the impact of the hyper-marketing of implants through hospitals and doctors.[124]

The aggressive promotion of human implant products in the United States and abroad utilize standard advertising techniques. In addition to utilizing hospitals and medical professionals as promoters, the product is being marketed for both security and recreational purposes. RFID implants are being publicized as a mere technological extension to the body-piercing trend that permits bodily integration with computers. A technology entrepreneur who volunteered for implants in both hands admitted to the New York Times "the symbolism of the tag is much more of a big deal as a social marker."[125] A website has been established in an effort to expand this social phenomenon of voluntary technological branding.[126] RFID implants are also being marketed for voluntary use by tavern patrons to avoid having to pay with cash or credit cards and for computer users who cannot remember their passwords.[127] Others, with an economic interest in the technology, have publicly volunteered to receive implants as part of a marketing strategy.[128]

At least one United States employer, an Ohio surveillance company, recently announced that two of its employees have received RFID implants for identification purposes.[129] However, it remains

---

[124] Rieback, Crispo & Tanenbaum, *supra* note 13.

[125] Anna Bahney, *High Tech, Under the Skin*, N.Y. TIMES, Feb. 2, 2006, at G1 (quoting Amal Graafstra, the first known person to independently have himself implanted with a chip).

[126] *The "Tagged" RFID implant forums*, http://tagged.kaos.gen.nz (last visited May 17, 2006).

[127] Chetna Purohit, *Technology Gets Under Clubbers' Skin*, CNN, June 9, 2004, http://www.cnn.com/2004/WORLD/europe/06/09/spain.club; Auslan Cramb, *Microchip to Allow Wallet-Free Drinking*, TELEGRAPH, Jan. 17, 2005, http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2005/01/17/nchip17.xml&sSheet=/news/2005/01/17/ixhome.html; Jamie McGeever, *Computer chips get under skin of enthusiasts*, REUTERS, Jan. 6, 2006, http://www.abc.net.au/news/newsitems/200601/s1542754.htm.

[128] Amal Graafstra, the owner of a technology company has received implants in both hands and has authored a book setting forth "cool projects" connected with RFID products. Bahney, *supra* note 123; McGeever, *supra* note 125. Law Professor Patricia J. Williams has questioned whether the announcement by VeriChip board member and former United States Secretary of Health and Human Services Tommy Thompson, of his intent to receive a GPS implant was related to a marketing strategy. Patricia J. Williams, *Telly-Tommy*, THE NATION, Aug. 15-22, 2005, at 13.

[129] Richard Waters, *US Group Implants Electronic Tags In Workers*, FIN. TIMES, Feb. 12, 2006, http://news.ft.com/cms/s/ec414700-9bf4-11da-8baa-0000779e2340.html.

unclear whether acceptance of the implants was mandated by the employer or was volitional.[130] In Mexico, the Verichip™ has been implanted in government officials for access to a secure government building and non-government volunteers have received implants in response to their fear of being kidnapped.[131] In 2005, Qustar Ltd. announced a plan to commence marketing to parents two models of implantable GPS devices aimed at responding to parental fears of child abductions.[132]

The development, marketing, and use of human RFID and GPS implants raise important legal and ethical issues.[133] Transferring the application of implant technology from animal chattel to humans, for the same purposes of identification and location control, creates the specter of geoslavery that may be violative of the Thirteenth Amendment. At present, however, the legal ramifications regarding human implants, including the legality of government or privately mandated implants, remains undeveloped.

It is improbable that a government program requiring human implants for non-criminals would be found to be lawful. Such a mandate would run afoul of Supreme Court due process jurisprudence and precedent establishing a constitutionally protected right to privacy against governmental intrusions into intimate personal affairs.[134] Mandated government intrusions into the human body implicate

---

[130] *Id.*

[131] Josh McHugh, *A Chip in Your Shoulder: Should I get an RFID Implant?*, SLATE, Nov. 10, 2004, http://www.slate.com/id/2109477.

[132] Quastar Ltd., *Ending the Tragedy of America's Missing Children*, http://64.233.161.104/search?q=cache:HFFSy7MngssJ:www.qustar.com/ver1/news/announces.php+implantable+gps+Qustar+Ltd.&hl=en&ct=clnk&cd=1 (last visited May 15, 2006).

[133] Edmundson, *supra* note 6; Dobson & Fisher, *supra* note 64.

[134] *See* Rochin v. California, 342 U.S. 165 (1952) (reversing conviction of the defendant based on evidence obtained through police action forcing him to vomit up drug capsules. The Court held that the evidence was obtained by methods volative of the Due Process Clause of the Fourteenth Amendment); Griswold v. Connecticut, 381 U.S. 479 (1965) (invalidating a state law prohibiting the use of contraceptive devices based on a constitutional right to privacy premised on various provisions of the Bill of Rights); Lawrence v. Texas, 539 U.S. 558 (2003) (invaliding a state anti-sodomy law as an unconstitutional abridgement of the right to privacy); *see also* Norman-Bloodsaw v. Lawrence Berkeley Laboratory, 135 F.3d 1260 (9th Cir. 1998) (recognizing a constitutional right to privacy cause of action against a federally-funded research laboratory that conducted unconsented testing for traits of sickle cell anemia, syphilis, and pregnancy).

substantial liberty interests protected under the Due Process Clause of the 14th Amendment.[135]

In *Rochin v. California*, the Court held that the police violated the due process rights of a drug suspect when they compelled an involuntary pumping of his stomach in order to seize two capsules containing drugs that he had swallowed.[136] Justice Felix Frankfurter, writing for the majority, emphasized the significance of coerced governmental intrusions into the body:

> This is conduct that shocks the conscience. Illegally breaking into the privacy of the petitioner, the struggle to open his mouth and remove what was there, the forcible extraction of his stomach's contents--this course of proceeding by agents of government to obtain evidence is bound to offend even hardened sensibilities. They are methods too close to the rack and the screw to permit of constitutional differentiation.[137]

Under the Fourth Amendment, the Court treats all physical intrusions by governmental officials into a human body as a search and seizure because it violates an expectation of privacy recognized by our society. This reasonable expectation of privacy against unwanted bodily intrusions is balanced against the articulated legitimate governmental interest to determine whether the search was unreasonable.[138] The application of this balancing test is very different when "special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable."[139] When the "special needs" concerns are not related to crime detection, courts will make a context-specific inquiry balancing the competing private and public interests.[140]

---

[135] *See* Washington v. Harper, 494 U.S. 210, 222 (1990); Cruzan v. Director, Mo. Dept. of Health, 497 U.S. 261, 278 (1990).

[136] *Rochin*, 342 U.S. at 172-173.

[137] *Id.* at 172.

[138] Skinner v. Railway Labor Executives Association, 489 U.S. 602, 619 (1989).

[139] Griffin v. Wisconsin, 483 U.S. 868, 873 (1987) (quoting New Jersey v. T.L.O., 469 U.S. 325, 351 (1985) (Blackman, J., concurring in judgment)).

[140] Chandler v. Miller, 520 U.S. 305, 314 (1997).

For example, mandatory drug and alcohol testing programs in employment and public schools have been upheld under the Fourth Amendment based on special safety needs that outweighed the reasonable expectation of privacy against such bodily intrusions.[141] In contrast, a state hospital policy, established with the aid of the police, under which non-consenting pregnant patients were subjected to urine drug tests and were subject to criminal prosecution if they tested positive for cocaine, was struck down as a violation of the Fourth Amendment.[142] In 1997, the Supreme Court invalidated on Fourth Amendment grounds a state law mandating that state political candidates certify that he or she has taken a drug test and that the result was negative.[143] In striking down the statute, the Supreme Court found that the State lacked any special need based on the lack of evidence demonstrating a drug problem among elected state officials or that they performed safety sensitive job duties.[144]

Based on the sustained nature of an implant's intrusion into the body, it is improbable that the courts, in most situations, would find that a special government interest outweighs the liberty and privacy interests protected under the United States Constitution. Nevertheless, police use of a scanner to obtain the identity of a lawfully stopped individual with an implant may not constitute a violation of the Fourth Amendment. In *Hiibel v. Sixth Judicial District Court*, the Supreme Court held that a Nevada law requiring a person, upon being stopped by the police, to identify himself to the police did not violate the Fourth Amendment.[145] In upholding the law, the Court reasoned that such a request for identification is reasonable in the context of a police stop.[146] It remains to be seen whether police scanning of an individual's RFID implant for identification information will be

---

[141] *Skinner v. Railway Labor Executives Association*, 489 U.S. at 618-621; National Treasury Employees Union v. Von Raab, 489 U.S. 656 (1989) (upholding the use of drug testing for government employees as a condition of promotion or transfer to certain positions directly involving drug interdiction or requiring the employee to carry a firearm); Vernonia School District 47J v. Acton, 515 U.S. 646 (1995) (upholding random drug testing for high school students participating in interscholastic sports).

[142] Ferguson v. City of Charleston, 532 U.S. 67 (2001).

[143] *Chandler*, 520 U.S. at 323.

[144] *Id.* at 321-322.

[145] Hiibel v. Sixth Judicial Circuit of Nevada, 542 U.S. 177 (2004).

[146] *Id.* at 188.

deemed by the courts to constitute an extension of the holding in *Hiibel* or be construed as a bodily intrusion subject to the Fourth Amendment.

Without new legislation banning the practice, the common law tort of assault and battery, as well as the Thirteenth Amendment, would form the bases for challenging privately mandated human tracking implants. In *Schloendorff v. Society of New York Hospital*, the New York Court of Appeals recognized that "[e]very human being of adult years and sound mind has a right to determine what shall be done with his own body."[147] When someone is subjected to unwanted non-emergency surgery, they have the right to sue for damages for assault.[148]

Mandated human RFID implants that contain confidential medical information may also violate the confidentiality provisions of the Health Insurance Portability and Accountability Act (HIPAA) and the Americans with Disabilities Act (ADA).[149] A mandate that medical information protected under HIPAA be made accessible through an RFID implant to anyone with an appropriate reader would violate HIPAA's confidential provisions.[150] To the extent that an employer mandates implants for employees containing confidential medical information would render the employer vulnerable to liability based on the ADA's confidentiality requirements with respect to medical records.[151]

For at least a decade, electronic wrist and ankle bracelets have been required as a condition of house arrest, probation, and parole to enable officials to keep track of the offenders in and outside the home. Individuals under house arrest, along with probationers and parolees, are granted "conditional liberty" subject to special and unique restrictions including a significantly reduced expectation of privacy.[152] Due to the limitations connected with the radial scope of RFID technology, electronic bracelets utilizing GPS technology are increasingly being utilized throughout the country.

---

[147] Schloendorff v. Society of New York, 105 N.E. 92, 93 (1914).

[148] *Id.*

[149] *See* 42 U.S.C. § 1320d-2; 42 U.S.C. § 12112(d) (2006).

[150] *Id.*

[151] *See* 29 C.F.R. §§ 1630.14(b)(1), (d)(1) (2006).

[152] Griffin v. Wisconsin, 483 U.S. 868, 874 (1987) (quoting Morrisey v. Brewer, 408 U.S. 471, 480 (1972)); *see* United States v. Knights, 534 U.S. 112, 119-120 (2001).

As a practical matter, most people convicted of a crime would prefer electronic location monitoring to incarceration. This alternative to prison serves various societal interests because it is less expensive and grants the offender a greater opportunity to engage in rehabilitative activities.

The criminal population most vulnerable to a potential program of mandated human tracking implants is those convicted of sex crimes. In Ohio, a county official and sheriff have stated their support for the use of implants to monitor ex-convicts.[153] Due to heightened fear regarding recidivism by sex offenders, various states have enacted or are considering laws mandating lifetime electronic location monitoring for sex offenders.[154] In Wisconsin, the cost for implementing a 24 hour GPS tracking system for sex offenders has been estimated at $477 million over 20 years.[155] It may be only a matter of time before elected officials begin calling for the use of tracking implants on many different types of criminal convicts.[156]

Whether the Court will deem the use of tracking implants for inmates and other convicts to be violative of due process remains to be seen. Even when prison officials intrude on substantial liberty interests of prisoners, the regulation will be upheld as long as it is "reasonably related to legitimate penological interests."[157]

Although electronic bracelets have been utilized successfully, the fact that they are less intrusive than electronic implants does not preclude the possibility that human electronic implants will be found to be reasonable under the Fourth Amendment when applied to

---

[153] Mary Lolli, *Official: Implant Chips Into Offenders*, CINCINNATI POST, Mar. 29, 2005, at A5.

[154] Jim McKay, *Electronic Tether*, GOV'T TECH., Feb. 2, 2006, http://www.govtech.net/magazine/channel_story.php/98310; Matthew Mosk, *A Lone Voice Against Sex Offender Bill*, WASH. POST, Mar. 25, 2006, at B1, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/03/24/AR2006032401918.html.

[155] Steven Walters, *GPS tracking sought for sex offenders*, MILWAUKEE J. SENTINEL, Mar. 30, 2006 *available at* http://www.jsonline.com/story/index.aspx?id=412260.

[156] State mandated location information regarding criminals can have gruesome consequences. In April 2006 two Maine sex offenders were murdered by an individual who located them through Maine's sex offender registry demonstrating that reduced location privacy can transform a perceived or actual human predator into prey. Emily Bazar, *Suspected shooter found sex offenders' homes on website*, USA TODAY, Apr. 18, 2006, *available at* http://www.usatoday.com/news/nation/2006-04-16-maine-shootings_x.htm.

[157] Washington v. Harper, 494 U.S. 210, 223-224 (quoting Turner v. Safley, 482 U.S. 78, 89 (1987)).

criminal offenders. In a series of Fourth Amendment decisions, the Supreme Court has been dismissive of arguments premised on the mere existence of less intrusive means.[158] Under the Fourth Amendment special needs and general balancing tests, federal courts have sustained state laws mandating the extraction of DNA samples from the bodies of various classes of convicted offenders to be utilized in a computerized DNA database.[159] In any challenge to possible future use of human implants on criminal offenders, strong national evidence will have to be presented to a court demonstrating the success of the less intrusive electronic bracelets along with evidence establishing that implanted GPS technology is not more accurate or reliable than data stemming from a bracelet.

As a practical matter, the best means of establishing informed public policy with respect to implant technology is through a deliberative legislative process on the national, state, and local levels along with informed and reasoned public debate. The article next discusses the congressional response to the development and use of other forms of human tracking technology over the past twenty years. The lack of substantial legislative movement in the field of tracking technology renders it unlikely that there will be a federal legislative response to human implants in the near future.

III. FEDERAL LEGISLATIVE RESPONSES TO HUMAN TRACKING AND CELLULAR TECHNOLOGY

In response to the development of electronic technology, Congress has enacted legislation placing certain restrictions on the use of tracking technologies by federal law enforcement. The protection of privacy against the use of various forms of new technologies, however, has not been a major congressional priority.

In 1986, Congress passed the Electronic Communications Privacy Act of 1986 ("ECPA"). The ECPA includes a specific provision regarding federal law enforcement use of mobile tracking devices to monitor the movement of an individual or object.[160] The purpose of

---

[158] *See* Illinois v. Lafayette, 462 U.S. 640, 647 (1983); United States v. Martinez-Fuerte, 428 U.S. 543, 556-557 n. 12 (1976).

[159] *See* Nicholas v. Goord, 430 F.3d 652, 671 (2d Cir. 2005); United States v. Kincade, 379 F.3d 813 (9th Cir. 2004) (en banc), *cert. denied,* 544 U.S. 924 (2005); Green v. Berge, 354 F.3d 675, 679 (7th Cir. 2004).

[160] 18 U.S.C. § 3117 (2006).

the law was jurisdictional in nature. It did not place any expressed substantive limits on the use of tracking devices, require the suppression of evidence for statutory violations, or provide for any privacy protections beyond those recognized under the Fourth Amendment.[161]

The ECPA does include statutory mandates requiring federal law enforcement to apply before a federal judge for issuance of a search warrant based on probable cause or a court order based on a lesser standard when it seeks the release of certain forms of subscriber information from a wireless company.[162] Title III of ECPA establishes procedures relating to the use of pen registers and trap/trace devices, commonly referred to as a caller identification system, by federal law enforcement to capture the phone numbers of outgoing and incoming calls.[163] In 1994, Congress enacted the Communications Assistance for Law Enforcement Act prohibiting wireless providers from disclosing "any information that may disclose the physical location of the subscriber" based on call-identification information acquired through the government's use of a pen register or trap/trace device.[164]

In 1999, Congress enacted the Wireless Communications and Public Safety Act that contains an express limitation on the use or disclosure by telecommunication companies of call location information regarding mobile service customers.[165] Litigation challenging the FCC regulations with respect to the nature of consumer authorization required for the disclosure of location information has substantially muddled the enforceability of this location privacy provision.[166] The unwillingness of the Federal

---

[161] *See* United States v. Forest, 355 F.3d 942, 950 (6th Cir. 2004); United States v. Gbemisola, 225 F.3d 753, 758 (D.C. Cir. 2000), *cert. denied*, 531 U.S. 1026 (2000*); In re* Application for Pen Register and Trap/Trace Device with Cell Site Location Auth., 396 F. Supp 2d 747, 751-753 (S.D. Tex. 2005); Otterberg, *supra* note 6, at 679.

[162] 18 U.S.C. §§ 2703(a)-(d) (2006).

[163] 18 U.S.C. §§ 3121-27 (2006).

[164] 18 U.S.C. §3122(b)(2) (2006); *In re* Application of the United States for an Order Authorizing the Installation and Use of a Pen Register and a Caller Identification System on Telephone Numbers [Sealed] and [sealed] the Production of Real Time Cell Site Information, 402 F. Supp 2d 597, 603 (D. Md. 2005) (quoting 47 U.S.C. § 1002(a)(2)).

[165] 47 U.S.C. § 222(f) (2006).

[166] *See* Edmundson, *supra* note 6, at 219-224; Brendan J. Koerner, *Your Cellphone Is A Homing Device*, LEGAL AFF., July/Aug. 2003, at 30.

Communication Commission to promulgate rules aimed at clarifying the scope of the statute's protection of customer location privacy may undermine confidence in the little known statutory provision.[167] Despite this continued lack of clarity related to consumer consent, United States District Court Magistrate Stephen William Smith has concluded that the statute places location information into "a special class of customer information, which can only be used or disclosed in an emergency situation, absent express prior consent by the customer. Based on this statute, a cell phone user may very well have an objectively reasonable expectation of privacy in his call location information."[168] Despite the lack of clarity in governing cellular tracking, these protections surpass the protections for consumers utilizing non-cellular forms of wireless products containing GPS technology, who are not currently protected by any statutory location privacy protections.[169]

The narrow contours of current federal concerns relating to privacy intrusions resulting from new technologies are confirmed by the provisions of the Video Voyeurism Prevention Act of 2004.[170] The bill amended the federal criminal law to prohibit the use of cell phone cameras and concealed miniature cameras on federal property to capture an image of the "private area" of a non-consenting individual.[171] The law was enacted without congressional hearings and was based on anecdotal evidence regarding the use of the new technology to post on the internet sexually explicit or provocative images secretly recorded in locker rooms and other undressing areas.[172]

In criminalizing the prurient use of new technology on federal property, Congress codified a very narrow definition of the reasonable expectation of privacy standard:

---

[167] *In the Matter of* Request by Cellular Telecommunications and Internet Association to Commence Rulemaking to Establish Fair Location Information Practices F.C.C. 02-208 (2002), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-02-208A1.pdf.

[168] *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F. Supp 2d at 757.

[169] Anne Broache, *Wireless Location Tracking Draws Privacy Questions*, CNET NEWS.COM, May 16, 2006, http://news.com.com/2100-1028_3-6072992.html.

[170] 18 U.S.C. § 1801 (2006).

[171] 18 U.S.C. § 1801(a), (b) (2006).

[172] H.R. REP. NO. 108-504, at 3 (2004), *as reprinted in* 2004 U.S.C.C.A.N. 3292, 3293.

> A) circumstances in which a reasonable person would believe that he or she could disrobe in privacy, without being concerned that an image of a private area of the individual was being captured; or
>
> B) circumstances in which a reasonable person would believe that a private area of the individual would not be visible to the public, regardless of whether that person is in a public or private place.[173]

The federal codification of this reasonable expectation of privacy standard without input during public hearings from those victimized by such privacy intrusions, legal scholars, prosecutors, criminal defense attorneys, and privacy advocates is indicative of the limited legislative concern regarding the impact of new technological devices on privacy.

In contrast to the congressional focus on the possible capture and use of sexual images obtained in federal buildings and parks, a bill introduced by Congressman Kendrick Meek on May 20, 2004 in the 108th Congress to require the designation of a senior official within the United States Office of Management of Budget as the chief privacy officer for the federal government, as well as the designation of privacy officers for every federal department, died after being referred to the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census.[174] Under the proposed legislation, the federal chief privacy officer would have been responsible for insuring that the technology utilized by the federal government did not erode privacy protections.[175]

Congress has also been resistant to enacting legislation aimed at placing limitations on the ability of employers to impose electronic workplace tracking. In 1993, the Privacy for Consumers and Workers Act was introduced in Congress seeking to set limitations on the use of tracking technology in the workplace, including mandating written

---

[173] 18 U.S.C. § 1801(b)(5)(A)-(B) (2006).

[174] Strengthening Homeland Innovation to Emphasize Liberty, Democracy, and Privacy Act, H.R. 4414, 108th Cong. (2004), *available at* http://www.govtrack.us/congress/bill.xpd?bill=h108-4414; *see* GovTrack.us, Status of H.R. 4414[108]: SHEILD Privacy Act, http://www.govtrack.us/congress/bill.xpd?bill=h108-4414 (last visited Apr. 10, 2006).

[175] H.R. 4414, § 3(b)(1).

notification to employees regarding the surveillance.[176] The bill died in committee.[177] One year later, in 2000, the Notice of Electronic Monitoring Act was introduced.[178] The proposed legislation sought to amend the ECPA to mandate employers to provide written notice to employees regarding employer use of tracking technology.[179] Congress never acted upon the bill.[180]

In the face of federal legislative inertia, along with adverse federal court decisions under the Fourth Amendment, it is far more likely that varied public policy solutions in the field of privacy and technology will be developed at the state level.

IV. STATE COMMON AND STATUTORY LAW RESPONSE TO ELECTRONIC HUMAN TRACKING

A. THE APPLICATION OF STATE TORT LAW

Since the 19th Century, various state courts have recognized common law invasion of privacy torts that may be applicable to the use of electronic tracking devices. There are four distinct privacy torts recognized today in many states: (a) unreasonable intrusion upon the seclusion of another; (b) appropriation of another's name or likeness; c) unreasonable publicity given to another's private life; (d) publicity that unreasonably places the other in a false light before the public.[181] Privacy torts grant individuals the right to bring a lawsuit for damages usually in state court against the person who invaded the individual's privacy.

---

[176] Jill Yung, *Big Brother IS Watching: How Employee Monitoring in 2004 Brought Orwell's 1984 to Life and What the Law Should Do About It*, 36 SETON HALL L. REV. 163, 205-206 (2005).

[177] *Id*. at 206.

[178] *Id*. at 207.

[179] *Id*.

[180] *Id.* at 208.

[181] RESTATEMENT (SECOND) OF TORTS §§ 652A-E (1977)*; see, e.g.*, Johnson v. Stewart, 854 So.2d 544, 547-548 (Ala. 2003); Hamberger v. Eastman, 206 A.2d 239, 241 (N.H. 1964).

The privacy tort with the strongest relevance to the use of location tracking devices is the intrusion on seclusion tort.[182] The Restatement (Second) of Torts § 652B defines the tort of intrusion on seclusion in the following manner:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.[183]

This privacy tort is not limited to the physical trespass into another person's home or other physical space. It has been found applicable to attempted eavesdropping on private conversations with or without the use of technological devices.[184]

The viability of this type of lawsuit challenging the *per se* use of electronic tracking devices to follow another person outside the home remains dubious.[185] Comment (c) to the Restatement (Second) of Torts § 652B states that there can not be liability for observing or photographing another person while he or she is walking on a public street because the person is not in seclusion.[186]

In 2005, the Connecticut Appellate Court issued the first appellate decision considering an intrusion upon seclusion claim based on the use of a GPS device.[187] In *Turner v. American Car Rental, Inc.*, a rental company had installed a global positioning system in its vehicles as a means of controlling and punishing drivers for exceeding a set speed limit.[188] Under the company's policy and practice, the vehicle's GPS receiver transmitted the speed and location of the

---

[182] *See* Waseem Karim, *The Privacy Implications of Personal Locators: Why You Should Think Twice Before Voluntarily Availing Yourself to GPS Monitoring*, 14 WASH. U.J.L. & POL'Y 485, 496-497 (2004); Aaron Renenger, *Satelitte Tracking and the Right to Privacy*, 53 HASTINGS L.J. 549, 558 (2002).

[183] RESTATEMENT (SECOND) OF TORTS § 652B (1977).

[184] *See Hamberger*, 206 A.2d at 241.

[185] Karim, *supra* note 182, at 497.

[186] RESTATEMENT (SECOND) OF TORTS § 652B cmt. c (1977).

[187] Turner v. American Car Rental, 884 A.2d 7 (Conn. App. Ct. 2005).

[188] *Id.* at 9.

vehicle to a monitoring company that in turn faxed the results to the rental company.[189] In its form lease, the company stated that each rental vehicle contained a GPS receiver and set as a contractual condition that each time the rented vehicle exceeded 79 miles per hour for two minutes or longer, the leaser would be fined $150.00.[190] In dismissing the invasion of privacy tort action, the Connecticut appellate court concluded that it was unaware of any legal precedent establishing that the installation of a GPS device in a car violates the privacy rights of the driver or that that driver has an expectation of privacy on a public highway.[191]

The Supreme Court's conclusion in *United States v. Knotts*, that there is no reasonable expectation of privacy with respect to one's location while driving,[192] led a United States District Court judge to dismiss an employee's intrusion upon seclusion claim against his employer for monitoring him through the installation of a GPS device in the company vehicle that the employee used during work and during non-work hours.[193]

In Illinois, an appellate court affirmed the dismissal of a class action lawsuit brought by cell phone users against a large cellular phone service company for intrusion upon seclusion based on the company providing, to a research firm, specific information regarding its cell phone customers, including their names, telephone numbers, addresses, and social security numbers.[194] The Illinois appellate court emphasized that in order to state a claim for intrusion upon seclusion, plaintiffs must allege private facts and that none of the information provided to the research company constituted private information.[195]

---

[189] Am. Car Rental v. Comm'r of Consumer Prot., 869 A.2d 1198, 1202 (Conn. 2005) (affirming state administrative sanctions against the same company for an unlawful liquidated damages provision contained in the rental agreement).

[190] *Id*. at 1201-1202.

[191] *Turner*, 884 A.2d at 11.

[192] United States v. Knotts, 460 U.S. 276, 281 (1983).

[193] Elgin v. St. Louis Coca-Cola Bottling Co., No. 4:05CV970, 2005 WL 3050633, at *4 (E.D. Mo. Nov. 14, 2005).

[194] Busse v. Motorola, 813 N.E.2d 1013, 1018 (Ill. App. Ct. 2004), *appeal denied*, 829 N.E.2d 786 (Ill. 2005).

[195] *Id*. at 1017; *see also* Nader v. General Motors, 255 N.E.2d 765, 769 (N.Y. 1970) (stating, "It should be emphasized that the mere gathering of information about a particular individual does not give rise to a cause of action under this theory. Privacy is invaded only if the

Similarly, an intrusion upon seclusion action in Ohio against an employer for videotape surveillance of an employee was dismissed because the videotaping was limited to the employee's public activities.[196]

In 2003, the New Hampshire Supreme Court affirmed the dismissal of an intrusion upon seclusion cause of action against an internet-based investigation and information service company that had obtained employment information about the plaintiff's daughter, Amy Boyer, by making a pre-textual call to Ms. Boyer.[197] After obtaining the information, the company provided it to a New Hampshire man named Liam Youens who had ordered it over the internet for $109.[198] After receiving the employment information from the company, Youens went to Ms. Boyer's workplace and shot her dead before he committed suicide.[199] In dismissing the mother's intrusion upon seclusion claim in *Remsburg v. Docusearch*, the New Hampshire Supreme Court specifically relied upon the public exposure exception to the right to privacy:

> A person's employment, where he lives, and where he works are exposures which we all must suffer. We have no reasonable expectation of privacy as to our identity or as to where we live or work. Our commuting to and from where

---

information sought is of a confidential nature and the defendant's conduct was unreasonably intrusive. Just as a common-law copyright is lost when material is published, so, too, there can be no invasion of privacy where the information sought is open to public view or has been voluntarily revealed to others.").

[196] York v. Gen. Elec., 759 N.E.2d 865 (Ohio Ct. App. 2001), *compare* Johnson v. Corporate Special Services, 602 So.2d 385, 388 (Ala. 1992) (holding that a special investigator hired by an employer to investigate an employee was not intrusion upon seclusion because the investigator did not monitor the employee within the employee's house), *and* Jackson v. Playboy Enterprises, 574 F. Supp. 10, 13 (S.D.Ohio 1983) (holding that the unconsented publication of a photograph taken in a public place did not create a claim for intrusion upon seclusion).

[197] Remsburg v. Docusearch, 816 A.2d 1001, 1009 (N.H. 2003). However, the court found merit to the plaintiff's state consumer protection claim against the company and remanded that claim to the lower court.

[198] *Id.* at 1005-06.

[199] *Id.* at 1006.

> we live and work is not done clandestinely and each place provides a facet of our total identity.[200]

Nevertheless, based on societal concerns regarding the dangers of stalking and identity theft in the new technological age, the New Hampshire court ruled that if criminal misconduct against a third person is sufficiently foreseeable, an investigator has a legal obligation to exercise reasonable care when disclosing that person's personal information to a client.[201]

B. STATE STATUTORY LIMITATIONS ON ELECTRONIC TRACKING DEVICES

Many states have enacted legislation aimed at restricting the use of electronic devices by members of the public and the police. Other states are considering similar limitations on the use of such devices in vehicles.[202] Most of these measures are aimed at creating new criminal prohibitions or procedures and expanding consumer protections with respect to rental companies. Due to the speed of technological change, the pace of legislative deliberations and the intricacy of the technology, these legislative measures have not included responses to human implants and cellular technology. Furthermore, state initiatives aimed at regulating location surveillance in the workplace have been unsuccessful.[203]

In response to court decisions upholding the constitutionality of the warrantless use of tracking devices by police, various states have enacted laws requiring law enforcement officials to apply to a court for a judicial warrant before installing such devices. Many of these statutes place specific time limits on the period of authorization.[204]

---

[200] *Id.* at 1009 (quoting Webb v. City of Shreveport, 371 So.2d 316, 319 (La. Ct. App. 1979).

[201] *Id.* at 1008.

[202] *See, e.g.*, *States Focus on 'Black Boxes' in Vehicles*, N.Y. TIMES, Mar. 27, 2005, at 16.

[203] Yung, supra note 174, at 209-210 (citing proposed laws in California, Massachusetts, Pennsylvania and other states that would have obligated employers to provide employees with written notice regarding the use of tracking devices).

[204] UTAH CODE ANN. § 77-23a-15.5(7) (2006); 18 PA. CONS. STAT. ANN. § 5761(e) (2005).

Other states have enacted laws regulating the use of tracking devices for criminal offenders subject to house arrest, probation, or parole.[205]

In 1998, California Legislature enacted a criminal statute prohibiting the use of "an electronic tracking device to determine the location or movement of a person."[206] The statute defines the phrase "electronic tracking device" as a device "attached to a vehicle or other movable thing that reveals its location or movement. . ."[207] The legislation contains two consent exceptions: when the owner, leasor, or leasee of a vehicle has consented to the use of the device and lawful use by law enforcement.[208] In addition, California has enacted consumer legislation limiting the use of GPS technology by rental companies. Under this law, rental companies are permitted to install GPS technology in their vehicles but are prohibited from using the electronic data to impose surcharges or fines.[209] Similar consumer legislation regarding rental companies has been enacted in other states.[210]

A recently enacted California law has embraced the use of RFID and biometric technologies as a means of reasonably accommodating the visually impaired. Under the legislation, future store point of sale devices for the purchase of goods and services used by consumers utilizing a personal identification number must have a specifically described tactile keypad or be equipped for the use of RFID, biometric, or other forms of technologically based personal identifiers.[211] The use of such technology is acceptable as long as it "provides the opportunity for the same degree of privacy input and output available to all individuals."[212]

Texas, in 1999, enacted a criminal law prohibiting the installation of an "electronic or mechanical tracking device on a motor vehicle

---

[205] W. VA. CODE ANN. § 62-11B-4 (2006); OKLA. STAT. ANN. tit. 57 §510.10 (2006), OHIO REV. CODE ANN. §2971.05(E) (2006); CAL. PENAL CODE §§ 1210.7, 3010 (West 2006).

[206] CAL. PENAL CODE § 637.7(a) (West 2006).

[207] *Id.* § 637.7(d).

[208] *Id.* §§ 637.7(b)-(c).

[209] CAL. CIV. CODE § 1936(p) (West 2006).

[210] Elizabeth C. Yen, *Rent A Car, Rent A Spy*, BUS. L. TODAY, July-Aug. 2005, at 59.

[211] CAL. FIN. CODE § 13082 (West 2006).

[212] *Id.* §§ 13082(a)(1), (2).

owned or leased by another person."[213] The Texas statute establishes a defense against criminal prosecutions for owner or leasee who has consented to the installation as well as law enforcement purposes.[214] A defense was also carved into the law for private investigators, who after obtaining written consent from the owner or leasee, can install the device in a vehicle or a in a private residential property.[215] The private investigator defense permits distrustful employers, spouses, or friends to utilize private detectives and GPS technology to track a third party.[216]

In addition, Texas codified restrictions on the distribution of biometric information in 2001. The Texas law prohibits the capturing of an individual's biometric identifier for commercial purposes without the consent of the individual.[217] The statute also places general restrictions on the sale, lease, and disclosure of biometric information.[218]

Washington's motor vehicle law permits drivers, on a voluntary basis, to submit biometric information to verify their identity when applying for a driver's license renewal or a duplicate of the license.[219] In crafting the statute, the Washington legislature placed explicit privacy safeguards on the handling of the biometric information by motor vehicle officials including prohibiting the release of the biometric information without court order and mandating other appropriate safeguards such as encryption.[220]

Montana's statutory limitation on electronic tracking devices was not made applicable to the tracking vehicles or humans. In 1999, the Montana legislature, acting based on the perceived needs of that state,

---

[213] TEX. PENAL CODE ANN. § 16.06(b) (Vernon 2003).

[214] *Id.* §§ 16.06(d)(1)-(3).

[215] *Id.* § 16.06(d)(4).

[216] Other states that have enacted specific criminal statutes limiting the use of electronic tracking devices in vehicles include Minnesota, Tennessee, and Hawaii. *See* MINN. STAT. ANN. § 626A.35 (2006); TENN. CODE ANN. § 39-13-606 (2005); HAW. REV. STAT. § 803-42 (1993).

[217] TEX. BUS. & COM. CODE ANN. § 35.50(b) (Vernon 2006).

[218] TEX. BUS. & COM. CODE ANN. § 35.50(c) (Vernon 2006).

[219] WASH. REV. CODE § 46.20.037 (2006).

[220] *Id.*

enacted a law that prohibits hunters from utilizing electronic devices "to track the motion of a game animal and relay information on the animal's movement to the hunter."[221]

The enactment of these laws has led to at least three criminal prosecutions against individuals who have unlawfully used an electronic device. In 2000, Robert Sullivan's wife commenced legal proceedings to end their marriage and she obtained a restraining order against him.[222] In response, Sullivan installed a GPS device in her car to keep track of her activities.[223] The device was repeatedly installed and removed by Sullivan to enable him to download the information.[224] Sullivan was successfully prosecuted and his conviction affirmed under Colorado's harassment by stalking statute that outlaws placing another person under surveillance in a manner that would cause serious emotional distress.[225]

In Wisconsin in 2002, a man pled no contest to stalking his former girlfriend by placing a GPS device under the hood of her car.[226] The plea resulted from the police obtaining the electronic records of his use of the technology.[227]

In Delaware, Nancy Biddle was prosecuted in 2005 for attaching a GPS tracking device to the frame of another woman's car for tracking purposes.[228] Ms. Biddle was convicted under Delaware's invasion of privacy criminal statute that prohibits the nonconsensual installation "in any private place" of a device for "observing, photographing,

---

[221] Mont. Code Ann. § 87-3-134 (2005).

[222] People v. Sullivan, 53 P.3d 1181, 1182 (Colo. Ct. App. 2002).

[223] *Id.*

[224] *Id.* at 1184.

[225] *Id.* at 1185; COLO. REV. STAT. ANN. § 18-9-111(4)(b)(III) (2006); *see also* O'Brien v. O'Brien, 899 So.2d 1133 (Dist. Ct. App. Fla. 2005) (in which the husband's email unlawfully obtained by wife in violation of Florida's electronic communications statute was excluded from evidence during their divorce trial); Evans v. Evans, 610 S.E.2d 264 (N.C. Ct. App. 2005) (in which the wife's sexually explicit e-mail was found admissible in divorce trial because they were not illegally intercepted by the husband).

[226] David A. Schumann, *Tracking Evidence with GPS Technology*, WIS. LAW., May 2004, at 8.

[227] *Id.*

[228] State v. Biddle, No. CRIM.A. 05-01-1052, 2005 WL 3073593, at *1 (Del. C.P. May 5, 2005).

recording, amplifying or broadcasting sounds or events in that place[.]"[229] After reviewing the conflicting federal and state case law on the question of whether an individual has a reasonable expectation of privacy while driving a vehicle, a Delaware judge convicted Ms. Biddle, noting that increased use of electronic devices is eroding personal liberty.[230]

V. THE USE OF TRACKING DEVICES IN EMPLOYMENT

Increasingly, throughout the United States, private and public sector employers are utilizing RFID, GPS, cellular technology, and biometrics as a means of monitoring work performance and employee location.[231]

In 2004, employers spent approximately $9 billion in technological monitoring devices for the workplace.[232] The recent announcement by an Ohio employer that two of its employees received RFID implants may be the beginning of a new ominous trend in American labor relations.[233]

In a survey of 24 major federal agencies, the United States Government Accountability Office (GAO) found that 13 agencies had implemented or had plans to implement RFID technology.[234] Increasingly, employers are replacing traditional time sheets and time clocks with biometric technology to monitor their employees' time and attendance.[235]

---

[229] DEL. CODE ANN. tit. 11, § 1335(a)(2) (2001); *Biddle*, 2005 WL 3073593, at *1.

[230] *Biddle*, 2005 WL 3073593, at *2.

[231] Charles Forelle, *On the Road Again, But Now the Boss Is Sitting Beside You*, WALL ST. J., May 14, 2004, at A1.

[232] Matthew Swaya & Stacey R. Eisenstein, *Emerging Technology In the Workplace*, 21 LAB. LAW. 1, 8 (2005).

[233] Waters, *supra* note 127.

[234] U.S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), GAO-05-551, INFORMATION SECURITY: RADIO FREQUENCY IDENTIFICATION TECHNOLOGY IN THE FEDERAL GOVERNMENT 13 (2005), *available at* http://gao.gov/new.items/d05551.pdf (the 13 agencies that utilized or intended to utilize the technology were focused on tracking both objects and people).

[235] Rosenzweig, Kochems & Schwartz, *supra* note 9, at 3; Stephanie Armour, *Biometrics to Imprint Job Site*, USA TODAY, Dec. 5, 2002, at B3.

Employers justify the implementation of such technology in the name of safety, security, efficiency, and productivity.[236] However, employer use of this new technology does not usually stem from empirical data demonstrating an increase in workplace fatalities and injuries, or a decrease in efficiency and productivity.

As a practical matter, employers already have at their disposal many other effective and less intrusive managerial tools to deal with safety concerns, security, and productivity: employee training; tachometers and odometers to measure speed, distance and mileage; intercom, two-way radios and cell phones; and supervisor and co-worker visual observations to ferret out employee misconduct. Electronic location monitoring enables employers to learn non-work related information including personal habits, tastes, and interests of employees. In addition, this information can become vulnerable to third-party access.[237]

Based on the lack of empirical or anecdotal evidence, there appears to be one central explanation for the growing use of human tracking technology in employment: an effort by employers to expand their power and domination over their workforce. Twenty years ago, Gary T. Marx and Sanford Sherizen recognized that employer use of electronic technology for employee monitoring is a modern means of implementing the management ideas of Frederick Taylor which are aimed at increasing productivity and maximizing employer profit.[238]

In order to avoid the stigma of being perceived as engaging in excessive surveillance, some employers will rely on pretexts to justify the use of tracking technology. Pretexts and secrecy are used to avoid a perception that the employer is using totalitarian tools or mistreating its employees.

Prior to the purchase and implementation of workplace tracking technology, it is rare for an employer to discuss with its employees the purpose and nature of the new form of surveillance. Without a union representing the employees, the employer has no legal obligation to discuss or negotiate changes in terms and conditions in employment including the implementation of tracking technology. Nevertheless,

---

[236] Yung, *supra* note 176, at 175-178.

[237] GAO, *supra* note 234, at 18; Rosenzweig, Kochems & Schwartz, *supra* note 9, at 7.

[238] Gary T. Marx & Sanford Sherizen, *Monitoring On the Job: How to Protect Privacy As Well As Property*, 89 TECH. REV. 63, 63-64 (1986).

advocates for the expansive use of the new technology encourage employers to be open and honest with their employees.[239]

An unusual public debate regarding the proposed implementation of tracking technology in employment took place in the City of Boston in 2004. On November 8, 2004, the Boston City Council conducted a legislative hearing to consider a proposed order to encourage the installation of GPS devices on Boston's 720 public school buses.[240] Councillor John M. Tobin, Jr., as chair of the Boston City Council Education Committee, scheduled the public hearing to examine the use of GPS technology as a means of keeping track of the location of students thereby enhancing their safety.[241] During the hearing, representatives from the school district, the bus company, and the bus drivers union debated the need and rationale for the implementation of GPS technology.[242] At the hearing, witnesses testified that the school district utilized a two-day radio system along with an electronic system that kept track of each bus's mileage and the time when it left and returned.[243] Supervisory road audits were used to monitor bus driver work performance.[244] The school bus company representative present at the hearing articulated various reasons to justify the use of a GPS system: provide back-up information in emergency situations, keep tabs on bus arrivals and departures, monitor bus speeds; insure

---

[239] Mark Roberti, *RFID and the Worker*, RFID J., Nov. 29, 2004, http://www.rfidjournal.com/article/view/1259.

[240] Heather Allen, *School Bus Drivers Protest GPS Plan*, B. GLOBE, Nov. 9, 2004, at B2.

[241] *Id.*; Steve Garfield, *Councillor Tobin to Propose Tracking System Aboard City's School Buses*, Sept. 21, 2004, www.votejohntobin.com/blog/PressRoom/_archives/2004/9/21/259566.html.

[242] Allen, *supra* note 240 (noting that at the hearing, the bus drivers' union vehemently questioned the motivation and legality of the City Council initiative. The hearing was held following the conclusion of private sector negotiations between the bus drivers' union and the bus company with respect to a new contract. During those negotiations, the bus company had placed on the table a proposal for the installation of GPS devices. Based on the union's strong opposition to the proposal, the company withdrew that proposal which enabled the parties to reach a tentative agreement for a new contract.).

[243] Videotape: Review of feasibility and cost of installation of global positioning system on school buses Before the Boston City Council Committee on Education (Boston City Council 2004) (on file with author) [hereinafter Boston City Council Hearing].

[244] *Id.*

bus drivers' adherence to set bus routes, and provide guidance in following those routes.[245]

In response, union officials and rank and file bus drivers refuted these alleged purposes.[246] The union president stated that the primary purpose for the bus company wanting the new technology was to be able to challenge the drivers' wages, which were based on the specific amount of time the drivers worked each day.[247] He explained that the surveillance system would not enable the company to know the reason for a bus delay or the modification of a bus route.[248] With respect to student safety, the primary reason given by City Councillors for supporting the resolution, various drivers argued that GPS technology could not provide data regarding which bus a student may be on or identify the specific location where a student exited.[249] They emphasized that the best means of insuring that students get on the correct bus and off at the correct stop would be through personal supervision by a bus monitor.[250] Finally, the bus drivers explained that a GPS device, like a two-way radio system, is subject to interference and mechanical breakdown. [251]

Although locating students was the articulated central rationale behind the Boston GPS legislation, no one at the three hour City Council hearing mentioned using RFID technology as a means of keeping track of students like other school districts.[252] A detached look at the articulated municipal need and the available technology should have led Boston officials to discuss the possible use of smart cards and RFID badges for students. The failure to consider the use of an RFID system for students suggests that student safety was the pretext for the proposed location scrutiny of Boston bus drivers.

---

[245] *Id.*

[246] *Id.*

[247] *Id.*

[248] *Id.*

[249] *Id.*

[250] *Id.*

[251] *Id.*

[252] *See* Matt Richtel, *A Student ID That Can Also Take Roll*, N.Y. TIMES, Nov. 17, 2004, at A24; Lisa Guernsey, *Where's Johnny? Smart Cards and Satellites Help Keep Track*, N.Y. TIMES, Aug. 3, 2005, at G7.

Alternatively, the lack of a discussion regarding the use of the alternative technology may be reflective of an uninformed and reactive approach to incorporating new technology in the workplace.

Another example of the use of a pretext to justify the installation of tracking technology was presented during a 2005 disciplinary arbitration when a small marketing company offered GPS data to justify an employee's termination.[253] In December 2003, the company secretly installed GPS devices in all of its company's vehicles.[254] During the arbitration, the company contended that the reason for installing the tracking technology was to enable supervisors to know where to contact employees by telephone.[255] The company claimed that the secret tracking technology would increase productivity over the prior practice of using cell phones or calling work locations.[256] The illogic of the company's rationale is self-evident. The secrecy connected with the installation showed that the GPS device was never intended to be a means of communication between supervisors and employees. Even with the availability of the device, supervisors still had to call employees on their cell phones or at the worksites.

A far more colorable explanation for the company's decision to begin using the tracking technology was an incident six months earlier when the company's owner discovered that a twenty-year employee, who was the subject of the arbitration, was missing at a worksite.[257] Subsequent GPS data along with visual verification demonstrated to the company that the same employee was at home when he was supposed to be working in the field.[258]

The breadth and secrecy of the company's implementation of tracking technology backfired. Although the arbitrator concluded that the employee was guilty of serious misconduct, the arbitrator vacated the termination and imposed a sixty-day suspension based on the company's failure to disclose to its workforce the installation and purpose of the GPS system.[259]

---

[253] *In re* Beverage Marketing, 120 Lab. Arb. Rep. (BNA) 1388 (2005) (Fagan, Arb.).

[254] *Id.*

[255] *Id.*

[256] *Id.*

[257] *Id.*

[258] *Id.*

[259] *Id.*

A much more targeted approach to the use of GPS technology was utilized by a Missouri bottling company seeking to investigate cash shortages from vending machines in a particular service area.[260] Rather than over-reacting by installing GPS devices in all company vehicles, the employer placed monitoring devices only in vehicles used by employees with access to the specific machines with reported shortfalls.[261] After the employee was cleared of wrongdoing, he received notification that during the investigation he had been tracked with GPS technology.[262]

The use of pretext and secrecy regarding the use of tracking technology is aimed at avoiding employee opposition. Based on the power of the tracking devices, it is not surprising that it has resulted in employee protests and demonstrations against what is perceived to be a substantial intrusion into employee privacy. In Massachusetts, both snowplow operators and bus drivers have engaged in collective action at legislative hearings to challenge the use of human tracking.[263] In New York City, cab drivers held a demonstration protesting an administrative mandate for the installation of GPS devices in all taxicabs.[264] It is reasonable to expect larger and more sustained protests if employers attempt to impose human implants as a condition of employment.

Employees and cabbies are not the only people protesting against the implementation of tracking devices. Parent protests in a school district in Sutter County, California resulted in the district withdrawing its plan to implement RFID tags for the monitoring of its students.[265]

---

[260] Elgin v. St. Louis Coca-Cola Bottling Co., No. 4:05CV970, 2005 WL 3050633, at *1 (E.D. Mo. Nov. 14, 2005).

[261] *Id.* at *1-2.

[262] *Id.*

[263] *See* Forelle, *supra* note 231; Yung, *supra* note 176, at 178. In addition to organized protests, the installation of tracking technology can lead to employees engaging in self-help. In 2003, employees of a New Jersey company rebelled by disabling recently installed GPS devices. Otis Elevator Company v. Local 1, Int'l Union of Elevator Constructors, No. 03 Civ. 8862, 2005 WL 2385849 (S.D.N.Y. Sept. 23, 2005). Similarly, in 2001, three days after a distribution company announced that it had installed GPS devices in all of its trucks, an employee deliberately disconnected the device. *In re* Superior Products, 116 Lab. Arb. Rep. (BNA) 1623 (2002) (Hockenberry, Arb.).

[264] Matt Friedman, *Cabbies Rally Against GPS Tracking Mandate*, NEWSDAY, Mar. 21, 2006, at A14.

[265] Greg Lucas, *Students Kept Under Surveillance at School*, S.F. CHRON., Feb. 10, 2005, at B1.

In addition to overt protests, human tracking can lead directly to demoralization, hostility and lower productivity among the most dedicated and motivated of employees.[266] Under real-time scrutiny, employees feel dehumanized and fear being disciplined based on inaccurate electronic data or employers misconstruing the data.[267] For example, after an ABC television station affiliate installed GPS tracking devices on the station's mobile trucks, an unnamed on-air reporter was quoted by New York Magazine as stating: "Let's just say people are pretty pissed off…We were never really consulted, and the whole Big Brother aspect has us uncomfortable."[268] A Long Island snowplow driver expressed similar sentiments when he told a newspaper reporter that: "They're tracking us like we're 5 years old…I'm very on edge."[269] The sense of anger and fear articulated by both the television reporter and snowplow driver underscores the demoralizing impact caused by electronic tracking in the workplace.

In addition to diminishing morale and productivity, implementation of computer-based time records has other potentially adverse consequences for employers. Electronic time records can be the primary evidence in establishing overtime compensation claims under the Fair Labor Standards Act and analogous state laws. In addition, such records may be highly probative in employment discrimination and other litigation where the time and location of specific alleged conduct, such as sexual harassment, is a central factual issue in dispute.

At present, employees have few legal rights against the implementation or use of tracking technology by their employers while performing work duties.[270] The scope of recognized employee freedoms while at work in the United States is quite limited. As the

---

[266] David Colker, *Go Ahead, Just Try to Disappear*, L.A. TIMES, Dec. 27, 2004, at A1 (quoting management professor Lucas Introna regarding the discontent caused by employer location tracking).

[267] Yung, *supra* note 174, at 177-178; NAKED CROWD, *supra* note 5, at 51.

[268] Selim Algar, *Spywitness News*, N.Y. MAG., Oct. 24, 2005, *available at* http:www.newyorkmetro.com/nymetro/news/people/columns/intelligencer/14804/index.html.

[269] Brandon Bain, *Workers object to Babylon's satellite tracking system*, NEWSDAY, Mar. 13, 2006, at A6, *available at* http://www.newsday.com/news/local/longisland/ny-ligps0313,0,5610948.story?coll=ny-li-bigpix.

[270] Gundars Kaupins & Robert Minch, *Legal and Ethical Implications of Employee Location Monitoring*, 38TH HAW. INT'L CONF. ON SYS. SCI. 2 (2005) (noting the lack of any laws in the United States limiting employee location monitoring).

United States Supreme Court has observed "[o]rdinarily, an employee consents to significant restrictions in his freedom of movement where necessary for his employment, and few are free to come and go as they please during working hours."[271]

The Oregon Supreme Court's 2004 decision in *State v. Meredith* is indicative of the narrow judicial treatment of location privacy for employees.[272] Sixteen years before, the same court had broadly interpreted the Oregon Constitution to prohibit the warrantless use by the police of a tracking transmitter attached to a car.[273] In contrast, in *State v. Meredith*, the same court held that the use of the same type of electronic tracking device placed on the employer's vehicle used by an employee to perform her job duties in a national forest did not require a warrant.[274] In reaching its decision, the court found that the employee "did not have a protected privacy interest in keeping her location and work-related activities concealed from the type of observation by her employer that the transmitter revealed."[275]

In *O'Connor v. Ortega*, the Supreme Court ruled that public employees have constitutional protections against unreasonable searches and seizures in the workplace.[276] The Fourth Amendment is implicated only when workplace realities establish that the employee had a reasonable expectation of privacy through the use of doors, locks and personal passwords.[277] The openness of an office to the public and other employees may result in an expectation of privacy being deemed unreasonable.[278]

In 2001, a federal appellate court ruled that a state employee had a reasonable expectation of privacy in the content contained in his

---

[271] Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 624-625 (1989); *see also* Immigration & Naturalization Service v. Delgado, 466 U.S. 210, 218 (1984).

[272] State v. Meredith, 96 P.3d 342 (Or. 2004).

[273] State v. Campbell, 759 P.2d 1040, 1049 (Or. 1988).

[274] *Meredith*, 96 P.3d at 346.

[275] *Id.*

[276] O'Connor v. Ortega, 480 U.S. 709, 717 (1987).

[277] *See id.*

[278] *Id.*

workplace computer.[279] In concluding that the employee had a reasonable expectation of privacy with regard to the office computer, the appellate court noted that that the employee occupied a private office and maintained exclusive use of the computer, desk, and filing cabinet.[280] Even with the establishment of a reasonable expectation of privacy, the appeals court found that the search of the employee's computer was reasonable because it was based on the employer's reasonable suspicion that it would uncover evidence of employee misconduct.[281]

The *O'Connor v. Ortega* legal standards will result in interesting future legal challenges to the use of human tracking devices in public employment. For example, the Supreme Court's *Karo* decision may form the basis for a successful challenge to a public employer utilizing certain RFID and other internal tracking technology that allows for location surveillance in private areas, such as employee bathrooms and break rooms, where employees have a reasonable expectation of privacy. Another important unresolved issue is whether the application of *Knotts*, *Karo*, and *O'Connor* analyses will lead to Fourth Amendment or state constitutional limitations on government employers using GPS technology in laptops, cell phones, and other devices that would permit monitoring of employee location and movement while in the home.

In the private sector, the primary national law granting employees certain limited statutory workplace freedom, especially the right to organize, is the National Labor Relations Act.[282] Under that law, employers are prohibited from engaging in surveillance of protected concerted conduct and are obligated to negotiate mandatory subjects

---

[279] Leventhal v. Knapek, 266 F.3d 64, 73-74 (2d Cir. 2001); *see also* United States v. Slanina, 283 F.3d 670, 676 (5th Cir. 2002) (in which the court held that use of passwords and locking office doors to deny access to computer files can create reasonable expectation of privacy); *but see* United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) (in which the court held that public employer's internet policy eliminated any reasonable expectation of privacy); United States v. Bailey, 272 F. Supp 2d 822, 836-837 (D. Neb. 2003) (in which the court held that the employee had no reasonable basis to believe activities on work computer were private based on the screen notification).

[280] *Leventhal*, 266 F.3d at 73.

[281] *Id.* at 75.

[282] 29 U.S.C. § 151 (2006).

of bargaining with a certified or recognized union regarding certain forms of employee surveillance.[283]

The information provided by human tracking devices can be a very powerful tool in an employer's effort to defeat a union organizing campaign. By having electronic access to the location of employees at all times, the employer can determine which employees have been meeting together during lunch hours and break time and which employees have visited the union's office.[284] As a practical matter, however, it may be very difficult for a union or employee to establish that an employer's alleged discriminatory conduct toward an employee was based on electronic tracking.

In September 2005, a New York federal judge rejected a union's effort to vacate an arbitrator's decision that had found that the employer had a right, under the union contract, to install GPS technology in company owned vehicles.[285] The contract contained language granting the employer the right to continually upgrade technology it uses and specified certain electronic devices being utilized by employees.[286] In 2002, the company decided to install the GPS technology in company vehicles driven by employees.[287] Employees reacted strongly to the installation of the GPS devices and their union challenged the employer's action through the contractual grievance procedure.[288] The arbitrator concluded that the contract language granted the employer the right to upgrade the technology it utilized.[289] In rejecting the union's effort to set aside the arbitrator's

---

[283] *See* Chester County Hosp., Case 4-CA-21243, 320 N.L.R.B. 604, 1995 WL 795603 (1995); Colgate-Palmolive Co., Case 9-CA-32158, 323 N.L.R.B. 515, 1997 WL 202232 (1997).

[284] *See* Kaupins & Minch, *supra* note 268, at 3 (noting that electronic tracking would enable employers to more effectively monitor distribution of union materials in the workplace); Yung, *supra* note 174, at 192-194 (discussing that employer electronic tracking also has the potential of running afoul of state laws that prohibit employers from discriminating against employees for their off-duty activities).

[285] Otis Elevator Co. v. Local 1, Int'l Union of Elevators, No. 03 Civ. 8862, 2005 WL 2385849, at *8 (S.D.N.Y. Sept. 23, 2005).

[286] *Id.* at *1.

[287] *Id.* at *2.

[288] *Id.*

[289] *Id.* at *3.

decision, the federal court noted that the contract granted the employer expansive authority to update the technology it utilizes.[290]

The National Labor Relation Board's General Counsel has issued an advice memorandum on the question of whether a trucking company was legally obligated to negotiate with the Teamsters' union prior to installing GPS technology in company vehicles.[291] The memorandum concluded that the company did not have to negotiate with the union because it constituted a replacement of a prior communications system.[292] Before the installation of the electronic system, the truck dispatcher utilized a two-way radio to communicate with drivers.[293] Throughout the day, at specific set times, the drivers were required to use the radio to communicate with the dispatcher.[294] In addition, log sheets had to be submitted by drivers at the end of their shift.[295] Although the new GPS technology provided the employer with substantially greater surveillance power and information than the prior two-way radio, including the ability to monitor break times, the General Counsel reached the conclusion that the GPS technology was equivalent to the radio system and did not constitute a significant change in employment.[296]

The six-year negotiated contract between the United Parcel Service and the Teamsters contains a clause limiting the ability of the employer to discipline employees based on data collected through the GPS device carried by its employees.[297] The contract states, "No

---

[290] *Id.* at *7.

[291] Roadway Express, Inc., Case 13-CA-39940-1 (Nat'l Labor Relations Board Apr. 15 2002), http://www.nlrb.gov/nlrb/shared_files/admemo/admemo/x041502_roadway.asp?bhcp=1.

[292] *Id.*

[293] *Id.*

[294] *Id.*

[295] *Id.*

[296] *Id.*

[297] The legal requirement that an employer negotiate the implementation of a new tracking technology is not absolute. In 1976, the National Labor Relations Board (NLRB) held that an employer had an unfettered right to impose a mechanical timekeeping system to replace a manual record keeping system without negotiating with the union because the new system was not viewed as being a change in the terms and conditions of employment. Rust Craft Broadcasting of N.Y., Case 3-CA-6221, 225 N.L.R.B. 327, 329, 1976 WL 7242, at *4 (June 29, 1976). Administrative law judges in the private and public sectors have applied this reasoning to conclude that employers can impose biometric systems unilaterally in the

employee shall be disciplined for exceeding personal time based on data received from the DIAD/IVIS or other information technology."[298]

In contrast, despite vocal employee opposition to the implementation of GPS technology in town vehicles in Babylon, New York, the Teamsters local representing those employees was unable to persuade the employer to agree to limitations on the employer's use of the technology.[299]

Negotiated contractual provisions depriving employers of the ability to utilize location tracking information in discipline fits into what Jeffrey Rosen has labeled the "control-use model" of regulating new forms of technology surveillance.[300] In light of the employer's power over its employees during work time, a negotiated provision limiting the use of human tracking in disciplinary cases is a regulatory victory for employees. It also undercuts a primary articulated purpose for using such technology, namely discovering and disciplining employees for misconduct. Nevertheless, this type of negotiated language has inherent weaknesses. It accepts employer electronic tracking during an employee's personal time and does not prohibit electronic surveillance after hours. The provision does not address the employer's use of inaccurate information stemming from improper settings or malfunction and does not set any boundaries relating to the employer obtaining personal information about the employees' non-work activities.[301]

VI. POTENTIAL LEGAL SOLUTIONS

Prior to the establishment of potential legal solutions to human tracking technology, our society needs to conduct a measured and

---

workplace as a replacement for prior manual time keeping systems. Res Care, Case 2-CA-32700, 2001 WL 1598700 (N.L.R.B. June 8, 2001); Cal. State Employees Ass'n v. California (Cal. Youth Auth.), No. SA-CE-1099-S, 23 P.E.R.C. 30,114 (June 1, 1999).

[298] National Master United Parcel Service Agreement for the Period of August 1, 2002 through July 31, 2008, Article 37(d), *available at* http://www.browncafe.net/public/upsnma/#NATIONAL.

[299] Bain, *supra* note 269.

[300] NAKED CROWD, *supra* note 5, at 199.

[301] *See* Kaupins & Minch, *supra* note 270, at 5 (citing unenforceable ethical considerations relating to an employer's intrusion into an employee's personal business as well as the inaccuracies that can stem from electronic data).

meaningful debate to reach a national or local consensus regarding the acceptable contours of privacy in the new technological age. Such discussions should be aimed at drawing a proper balance between liberty, security, individual rights, and property rights. A reexamination of the reasonable expectation test should be explored during such a dialogue along with the issue of whether there is a societal consensus that exterior exposure should constitute the end of protected privacy.

Reliance on public fears perpetuated by the mass media, and marketing schemes aimed at responding to such fears, is not a formula for the development of reasoned public policy. Similarly, horrific acts perpetuated by the use of tracking devices should not be the only catalyst for modification of public policy regarding new technologies.

Gary T. Marx's suggestion that the use of new powerful surveillance tools may decrease or be modified if managers and corporate executives were equally subject to such surveillance remains untested.[302] Jeffrey Rosen has rejected the notion that ubiquitous technological transparency constitutes an adequate or appropriate means of balancing liberty with security.[303] Nevertheless, those advocating for the implementation of human tracking technology on others do not necessarily want to be subject to the same level of scrutiny. During the rare public debate in the Boston City Council regarding GPS technology in employment, the chief shop steward for the union representing the school bus drivers asked Councilor Tobin how he would react if his manager or boss monitored his every move through GPS surveillance.[304] Rather than providing a reflective answer regarding his own subjective sense of personal autonomy, the Councilor responded angrily asserting that his constituents would be able to vote for or against him in the next election.[305]

The question of location transparency for public officials and corporate managers remains unexplored. In developing and considering remedial legislation, it may be beneficial for a public official to agree to subject him or herself to location tracking for a day or week. A well-publicized experiment involving a public figure wearing a GPS device would lead to a greater understanding regarding

---

[302] Gary T. Marx, *Let's Eavesdrop On Managers*, COMPUTERWORLD, April 20, 1992, at 29.

[303] NAKED CROWD, *supra* note 5, at 194-199.

[304] Boston City Council Hearing, *supra* note 243.

[305] *Id.*

the power of the technology as well as potential legal changes needed to protect individual privacy. There is precedent for such an experiment. Companies are promoting tracking implants through publicity surrounding individuals who have consented to human implant. Public exposure to the results of technological tracking would enhance the debate regarding the use of the technology.

The negative reaction to the United States State Department's proposed rule regarding the introduction of an electronic passport program supports the conclusion that there is growing public support for limitations on new tracking technology. In the State Department's October 25, 2006 report announcing its final rule, it acknowledged that 98.5% of those who commented opposed electronic passports primarily on privacy and security grounds.[306] Despite such documented concerns, the Department determined that by October 2006 virtually all United States passports would contain a 64KB microchip capable of storing both data and biometric indicators.[307] Cognizant of the level of public opposition, the Department agreed that it would not require biometric indicators in the passport microchips until after a new rule is proposed and it obtains additional public comment.[308]

In May, 2006, an advisory subcommittee to the United States Department of Homeland Security issued an interim report recommending against the use of RFID technology to track and identify people.[309] The ability of the government to track and profile individuals without notice was one of the reasons for the subcommittee's recommendations.[310]

Based on the slow congressional response to the development of new technologies and the current political climate, it is unlikely that federal remedial legislation limiting human tracking technology will be enacted in the near future. In fact, an explicit policy agenda item for the Senate Republican High Tech Task Force in the 109th Congress is

---

[306] Electronic Passports: Final Rule, 70 Fed. Reg. 61,553, 61,553 (Oct. 25, 2005) (to be codified at 22 C.F.R. pt. 51), *available at* http://edocket.access.gpo.gov/2005/05-21284.htm.

[307] *Id.*

[308] *Id.*

[309] DEP'T OF HOMELAND SEC. EMERGING APPLICATIONS AND TECH. SUBCOMM., THE USE OF RFID FOR HUMAN IDENTIFICATION (2006), www.dhs.gov/dhspublic/interweb/assetlibrary/privacy_advcom_rpt_rfid_draft.pdf.

[310] *Id.* at 7-9.

to avoid what it has termed premature regulation of RFID technology.[311] Significantly, absent from the task force's agenda are GPS technology, location privacy protections, and regulation of human microchip implants.[312] In contrast, in 2005, Congress enacted legislation establishing and funding a national RFID animal microchip system for domestic pets.[313] It is possible, however, that rapid and reactive federal legislation regarding human tracking technology may be enacted following a well-publicized crime or tragedy or due to public fear caused by the abuse or misuse of tracking technology.

An alternative to emotive legislative responses to important privacy issues would be the establishment of a federal privacy commissioner or privacy commission, similar to governmental offices established in Canada and Australia, to study and analyze new technologies and provide Congress with suggested remedies. Although Congress did not act on the proposed 2004 legislation that would have created such an office, a federal chief privacy officer or commission would substantially assist the federal government, Congress, and the public in analyzing, understanding, and responding to potential privacy intrusions associated with new technologies. The European Union has already created a working group, known as the Article 29 Data Protection Working Party, which has closely examined privacy and data security issues associated with RFID technology.[314] In the United States, a similar pro-active response to technological developments would assist in the establishment of sober and balanced federal legislation relating to privacy and new technologies.

---

[311] Senate Republican High Tech Task Force, *Policy Agenda*, http://republican.senate.gov/httf/index.cfm?FuseAction=PolicyAgenda.Home.

[312] *Id.*

[313] Anne Eisenberg, *For the Fretting Pet Owner, a Wireless Distress Signal*, N.Y. TIMES, July 15, 2004, *available at* http://www.nytimes.com/2004/07/15/technology/circuits/15next.html?ex=1247630400&en=68121d87ca4dd70d&ei=5090&partner=rssuserland; Kathleen Megan, *GPS Designed to Find Lost Pets, Notify Owners*, MIAMI HERALD, Feb. 12, 2006, *available at* http://www.miami.com/mld/miamiherald/living/home/pets/13843615.htm. The Schering-Plough Animal Health Corporation markets the HomeAgain® pet recovery service that utilizes RFID implants. See HomeAgain® Pet Recovery Service, HomeAgain Information Center, http://www.homeagainpets.com/.

[314] Article 29 Data Protection Working Party, *Working Document on Data Protection Issues Related to RFID Technology*, Jan. 19, 2005, http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2005_en.htm.

However, it is far more probable that a majority in the current Congress will continue to defer to the marketplace for potential corrective action aimed at avoiding privacy intrusions. Such deferral is reflective of contemporary deregulation ideology and assumes that there is more profit to be made in protecting privacy than in collecting, using, and distributing location and other personal information. Although voluntary corporate initiated policies can aid in the protection of privacy, as well as increase profits through consumer good will, sole reliance on marketplace privacy solutions constitutes a public policy recipe for disaster.[315]

In addition, sole reliance on litigation in federal courts aimed at establishing constitutional protections against human tracking would be similarly misplaced. Based on the reasonable expectation of privacy test, along with precedents such as *Knotts*, it is doubtful that the Supreme Court will find that the use of newer and more powerful technologies to track public location and movement is subject to the Fourth Amendment. To the extent that new tracking technologies involve monitoring within the home, *Karo* and *Kyllo* suggest that Fourth Amendment standards would be applicable. However, law enforcement and public employers deserve more than post-hoc federal guidance relating to the constitutional dangers connected with the use of portable tracking devices contained in cell phones and laptops that can lead to unlawful location monitoring within a home. The computerized nature of GPS and cellular technology may result in the transition from constitutional public monitoring to unconstitutional surveillance within a home without real-time human supervision.

Since the development of human tracking devices, state legislatures and courts have been far more responsive to the privacy implications of such technology. State legislative initiatives have been aimed at criminalizing certain use of tracking technology, establishing judicial oversight over the police use of tracking devices, and extending consumer protections against the use of such technology in rented vehicles.

Based on the speed of technological change, states should also consider establishing a privacy commissioner or legislative commission with the authority to study technological developments and provide guidance regarding potential state legislative responses to a particular technology. Reports issued by Ontario Information and Privacy Commissioner Ann Cavoukian regarding the privacy implications of biometrics and RFID technology demonstrate the

---

[315] *See* Allan Holmes, *The Profits in Privacy*, CIO MAG., Mar. 15, 2006, at 64.

valuable role that such local government offices can play in developing public policy.[316] A state privacy commissioner or commission would aid in determining whether current state laws restricting the use of electronic tracking devices should be amended to regulate human implants as well as tracking devices attached to personal objects other than vehicles. States also need to reexamine their common law or statutory privacy causes of action to determine whether and to what extent lawsuits for damages and injunctive relief should be permitted for unwanted electronic location surveillance in public or in the home. In addition, serious consideration needs to be given to amending current state law to include prohibitions against the sale or distribution of location information to third parties from wireless products that are not subject to the Wireless Communications and Public Safety Act of 1999. Similarly, restrictions should be explored with respect to the distribution and sale of personal information emanating from RFID and biometric technology. Finally, another means of checking the potential abuse of tracking technology would be to subject tracking devices to state licensing regulation.

The need for careful legislative deliberation is particularly urgent in the area of human implants where the adverse social consequences of such devices have not been examined. The use of human implants is ripe for abuse and constitutes the most likely technological means for imposing geoslavery. State regulatory schemes and procedures have been enacted in some states regarding the implantation of microchips in dangerous dogs. It is a testament to the differing speeds of change between technology and the law that dangerous dogs in states such as Colorado have clearer procedural protections against mandatory implants than humans.[317] Although many states regulate more benign intrusions into the human body, such as tattooing and body piercing, regulations regarding human implants have not been promulgated. A prohibition or regulation regarding human implants should be carefully examined to properly weigh the varying interests associated with the technology. In determining whether to ban human implants, an examination should take place regarding whether the availability of bracelets, cards, and badges with encoded information

---

[316] *See, e.g.*, Ann Cavoukian, *Privacy and Biometrics*, INFORMATION AND PRIVACY COMMISSIONER/ONTARIO, Sept. 1999, http://www.ipc.on.ca/userfiles/page_attachments/pri-biom.pdf; Ann Cavoukian, *Tag, You're It: Privacy Implications of Radio Frequency Identification (RFID) Technology*, INFORMATION AND PRIVACY COMMISSIONER/ONTARIO, Feb. 2004, http://www.ipc.on.ca/docs/rfid.pdf.

[317] *See* COLO. REV. STAT. § 18-9-204.5(3)(E.5) (2006).

meet the same needs as implants. In addition, the substantive distinction between information obtainable from identification-based RFID implants and location-based GPS implants needs to be explored in developing state public policy in this area. At minimum, state restrictions should ban mandatory human implants without a court order following a due process hearing before a state judge with the burden of evidentiary proof being placed on the individual or entity seeking to impose a mandatory implant. In addition, states should debate and consider legislation banning mandatory GPS human implants. Finally, any state regulatory scheme that permits the voluntary use of human implants should require informed consent with respect to the nature of the implant, the risk of privacy intrusions associated with the implant and the means of removing the implant.

In the area of employment, state or local legislative initiatives may include a complete ban on human implants, a mandate for informed employee consent prior to the implementation of human tracking, written notice to employees regarding the surveillance, limitations on the daily period when surveillance would be permissible, specific legal sanctions for employers who utilize the technology for unlawful discriminatory purposes or to intrude on personal privacy, or a prohibition against employers sharing the electronic data with third parties. The need for such legislative action is particularly important based on the growing portability of tracking devices that enables an employer to monitor an employee while working or not working and within the employee's own dwelling. Such initiatives should be considered after careful legislative examination of the technology and a determination regarding the scope of protected employee personal privacy during and after working hours.

To the extent that fear justifies imposing electronic tracking on children and infirm elderly parents, a state requirement for judicial intervention or licensing may be an appropriate response. Courts already have been granted the power and jurisdiction to deal with children in need of supervision and mentally infirm individuals needing guardians. Placing a judicial or regulatory check on electronic tracking of children and the ill may provide a balanced means of permitting a technological response to rational or irrational fears while protecting personal privacy.

In the absence of or as an alternative to remedial legislation, industry groups and privacy advocates have been working on establishing voluntary, industry-wide standards to protect against inappropriate intrusions into individual privacy. On May 1, 2006, the Center for Democracy and Technology announced interim draft

guidelines prepared by a working group relating to the privacy implications of RFID technology.[318] Similarly, in the United Kingdom, Codes of Practice have been established for various forms of location based services.[319] Although "self-regulation" based on industry standards and guidelines has some benefits, they lack necessary safeguards including enforcement tools. Nevertheless, experiences connected with the development, implementation, and application of industry standards may assist in the formulation of future remedial legislation. Finally, another non-regulatory means of protecting privacy against human tracking would be modifications to the actual technology that may include an ability to turn the tracking device off or a signal indicating that the tracking component of the device has been deactivated.

In conclusion, the explosive growth of human tracking technology in the past two decades calls for a deliberative reexamination of our society's concepts of individual autonomy and the scope of protected privacy. The best means of reaching a societal consensus is through sober examination, deliberations, and debate with respect to the nature of new and developing technologies and the impact it has on our concepts of privacy. Through such a dialogue, an appropriate legal framework can be established to insure a reasonable balance between conflicting interests associated with the technology.

---

318 Center for Democracy and Technology, *CDT Working Group on RFID: Privacy Best Practices for Deployment of RFID Technology*, http://www.cdt.org/privacy/20060501rfid-best-practices.php (last visited May 18, 2006).

[319] Orange, *Our Commitment to You*, http://www.orange.co.uk/about/regulatory_affairs.html (last visited May 18, 2006).