SYMPOSIUM

THE IMPACT OF EMERGING TECHNOLOGIES IN THE WORKPLACE: WHO'S WATCHING THE MAN (WHO'S WATCHING ME)?†

William A. Herbert & Amelia K. Tuminaro[*]

Throughout the United States and most industrialized countries, private and public sector employers are purchasing and implementing new advanced technologies that enhance the monitoring of security and productivity while substantially increasing the level of intrusion into employee privacy. Like most new products, emerging technologies are marketed with an emphasis on the potential benefits but notably without regard to possible negative consequences for the workforce. As noted in a report prepared by the Union Network International[1] ("UNI") on contemporary workplace surveillance, employers often blindly adopt technological software capabilities without considering their adverse impacts.[2]

† An earlier version of this article was presented at the New York State Bar Association Labor and Employment Law/Municipal Law Section Fall Meeting on September 15-17, 2006 and is used with permission. The title is borrowed with permission from a 1982 song by songwriter Si Kahn. SI KAHN, *Who's Watching the Man?*, *on* DOING MY JOB (Flying Fish Records 1982); *see also* Si Kahn, http://www.sikahn.com/ (last visited Dec. 26, 2008).

* Mr. Herbert currently serves as Deputy Chair and Counsel for the New York State Public Employment Relations Board ("PERB") and Ms. Tuminaro is now an Associate with a New York City labor and employment law firm. The opinions expressed in this article reflect the personal views of the authors.

1. UNI is "the global union for skills and services," an organization comprised of 900 unions, representing 20 million members worldwide. UNI Global Union, http://www.union-network.org/ (last visited Nov. 7, 2008).

2. *See* ANDREW BIBBY, UNI GLOBAL UNION, YOU'RE BEING FOLLOWED: ELECTRONIC MONITORING AND SURVEILLANCE IN THE WORKPLACE 3-4 (2006), *available at* http://www.union-network.org/uniflashes.nsf/unireport?openpage (follow "Surveillance-en.pdf" hyperlink).

Employer implementation of new technologies is rationalized as a managerial prerogative aimed at increasing efficiency, tracking employees, and monitoring employer-owned property.[3] Studies reported in the New York Times demonstrate, however, that workplace technologies that encourage and facilitate multitasking often result in increased errors and lower productivity.[4] As columnist Ellen Goodman has observed, "[w]hen the chief product of 'productivity' is a bumper crop of mistakes and the primary 'shortcut' has become a leap to conclusions, we finally have a strong reason to push back against the clock."[5]

In addition, employers often ignore the adverse consequences to employee morale and occupational health from the impact of such technologies.[6] Technologies with expansive surveillance capabilities can lead to stress, alienation, and dehumanization of the workforce, resulting in unintended decreases in worker productivity and job satisfaction.[7] Business Ethics Professor James Hoopes has warned that the intensity of new technological surveillance may result in an increase in "management by stress."[8] The introduction and application of new workplace surveillance technologies may exasperate employee fears and tensions caused by the increasingly dire economic news stemming from the current recession.[9]

Overuse of e-mail and portable communication devices containing tracking technology, such as BlackBerrys, can intensify work related stress and anxieties. A lengthy disruption in BlackBerry service in April 2007 resulted in emotional reactions and even paranoia among some BlackBerry users.[10] Harvard University Clinical Associate Professor of Psychiatry John Ratey has proposed a new label—"acquired attention

3. *See id.* at 4.

4. Steve Lohr, *Slow Down, Brave Multitasker, And Don't Read This in Traffic*, N.Y. TIMES, Mar. 25, 2007, at 1.

5. Ellen Goodman, *Blogs a Shortcut to a Minefield of Errors*, TIMES UNION, Apr. 4, 2007, at A9.

6. BIBBY, *supra* note 2, at 33-34. *See also* CWA on the Issues, Occupational Stress & the Workplace, http://www.cwa-union.org/issues/osh/articles/page.jsp?itemID=27339172 (last visited Dec. 26, 2008) (connecting electronic performance monitoring and stress' adverse consequences).

7. BIBBY, *supra* note 2, at 34-36. *See* James Hoopes, *The Dehumanized Employee*, CIO MAG., Feb. 4, 2005, *available at* http://www.cio.com.au/index.php/id;451554300; CWA on the Issues, *supra* note 6 (describing the hazards of occupational stress).

8. Hoopes, *supra* note 7.

9. *See* Edmund L. Andrews, *Officials Vow to Act Amid Signs of Long Recession*, N.Y. TIMES, Dec. 2, 2008, at A1, *available at* http://www.nytimes.com/2008/12/02/business/economy/02econ.html?ref=business.

10. Brad Stone, *Bereft of BlackBerrys, the Untethered Make Do*, N.Y. TIMES, Apr. 19, 2007, http://www.nytimes.com/2007/04/19/technology/19blackberry.html?ref=technology.

deficit disorder"—to describe a psychological disorder resulting from the addictive qualities associated with the use of various communication devices such as BlackBerrys.[11] In an article reporting on the fall-out from the BlackBerry blackout of 2007, Dr. Ratey is quoted as stating: "I liken it to a drug . . . . Drug addicts don't think; they just start moving. Like moving for your BlackBerry."[12] According to Dr. Ratey, the treatment for addiction to technology will be as difficult as treating such ailments as food addiction.[13] Although the psychological impact of the BlackBerry disruption has raised awareness regarding technologically based workplace stress and addiction, the adverse impact of sophisticated employment-related surveillance technology on both employees and supervisors remains largely unexamined.[14]

The growth of occupational stress caused, in part, from the introduction of new workplace technologies has led some labor unions to adopt specific strategies to respond to the problem.[15] These strategies include: collective bargaining demands, worker education and union activist training, legislative initiatives, union-initiated stress surveys, and inspections and investigations of workplaces.[16]

Over thirty years ago, in *NLRB v. J. Weingarten, Inc.*,[17] the U.S. Supreme Court recognized that the use of new technologies increased employee anxiety, thereby justifying the National Labor Relations Board's ("NLRB") conclusion that employees have a statutory right to union representation during a disciplinary interrogation.[18]

Although emerging technologies can dehumanize, they also have the potential to benefit both employers and employees by making the workplace safer.[19] For example, the Federal Mine Safety and Health Administration has approved the use of a wireless tracking system in mines aimed at protecting miner safety.[20]

11. Matt Richtel, *It Don't Mean a Thing if You Ain't Got That Ping*, N.Y. TIMES, Apr. 22, 2007, http://www.nytimes.com/2007/04/22/weekinreview/22richtel.html?ref=technology.

12. *Id.*

13. *Id.*

14. *See generally id.*; BIBBY, *supra* note 2, at 31-32. In addition, prior to implementing surveillance technologies, employers frequently fail to consider the potential negative legal consequences that such computer-based information may have in the context of litigation. The computerized informational fruit of such technologies may be highly probative in wage and hour litigation and investigations along with other forms of employment litigation.

15. CWA on the Issues, *supra* note 6.

16. *Id.*

17. 420 U.S. 251 (1975).

18. *Id.* at 253, 265 n.10.

19. BIBBY, *supra* note 2, at 14.

20. Mike Gorrell, *Technology could help mine safety*, SALT LAKE TRIB., Feb. 1, 2008.

Without substantive limitations on their use, these technologies can create a sizeable imbalance between employer surveillance and the reasonable expectations of employees that they will not be subject to perpetual real-time monitoring. Such a disparity may lead to employee demoralization along with a possible resurgence in employee activism.

This article will examine the legal and policy issues, and practical consequences connected with certain emerging technologies in the workplace. These modern technologies, defined in each section below, are: mandatory genetic testing for disease and the collection of DNA samples for employee identification purposes,[21] global positioning systems ("GPS"),[22] radio frequency identification ("RFID"),[23] and biometrics.[24] While the privacy and productivity implications of e-mail and Internet use by employees are immense, this article will not discuss the legal and policy questions connected with those technologies.

Major advances in computer and telecommunications technology have radically reshaped the workday, eroded the separation between work and home, and further compressed available leisure time.[25] Such technologies have enabled the development of what Professor Katherine V.W. Stone has characterized as boundaryless workplaces.[26] In addition, various new technologies empower employers with surveillance capabilities to monitor and study employees even while not at work. Humberto Moran, from the British group Open Source Innovation, has observed, "[t]he bottom line is that secret surveillance is a strong source of power, highlighting the need to 'watch the watchers.'"[27]

As Professor Michael Selmi has recognized, there is a fundamental tension between the still vibrant employment at-will doctrine in many States and efforts to establish a legally cognizable zone of protected privacy for workers.[28] At the same time, the confluence of diminished union density in the United States, the growth of decentralized

21. *See infra* Part A.

22. *See infra* Part B.

23. *See infra* Part C.

24. *See infra* Part D.

25. During the earlier stages of the telecommunications and personal computer revolutions, Harvard University Professor Juliet B. Schor highlighted the already steady decline of leisure time for the American workforce. *See* JULIET B. SCHOR, THE OVERWORKED AMERICAN: THE UNEXPECTED DECLINE OF LEISURE 22-23 (1991).

26. *See* Katherine V.W. Stone, *Employee Representation in the Boundaryless Workplace*, 77 CHI.-KENT L. REV. 773, 773-74 (2002).

27. Humberto Moran, *Privacy-friendly RFID?*, ZDNET UK, May 22, 2006, http://opinion.zdnet.co.uk/comment/0,1000002138,39270505,00.htm.

28. Michael Selmi, *Privacy for the Working Class: Public Work and Private Lives*, 66 LA. L. REV. 1035, 1036 (2006).

workplaces, and the development of sophisticated tracking technology have accentuated the importance of individual worker privacy and the need for examining additional regulatory protections in the workplace.[29] The continued vibrancy of the at-will doctrine, despite the extraordinary transformation of the American economy since the nineteenth century, suggests that the movement of Benjamin N. Cardozo's metaphorical common law glacier may have stopped north of the Adirondacks.[30] The increase in economic insecurity caused by the present worldwide recession may be a catalyst for a reexamination of the common law doctrine, or such fears may result in a greater willingness to accept, without objection, increased workplace surveillance in exchange for continued employment.

The use of surveillance tools to monitor employees is not a new phenomenon. As Massachusetts Institute of Technology ("MIT") Professor Gary T. Marx has noted, in the late eighteenth century, philosopher Jeremy Bentham published *Panopticon or the Inspection House*, in which he described structures that would enable constant transparency of prisoners and factory employees.[31] Similarly, Frederick Taylor's work a century ago established a system of tests for measuring employee actions at work.[32] Bentham's parallel between penal surveillance and employer surveillance remains relevant to contemporary technology-based transparency: presently, law enforcement officials and employers are simultaneously introducing the same technologies for tracking and identification purposes.[33]

29. *Id.* at 1036-37, 1041-42.

30. BENJAMIN N. CARDOZO, THE NATURE OF THE JUDICIAL PROCESS, 25 (1921). *See* Horn v. N.Y. Times, 100 N.Y.2d 85, 90-95 (2003) (reaffirming New York's common law at-will doctrine and emphasizing the narrowness of any judicially recognized exception); Goldman v. White Plains Ctr. for Nursing Care, LLC, 11 N.Y.3d 173, 177 (2008) (distinguishing nineteenth century case law applying a common law presumption that parties intend to renew an employment agreement for an additional year when an employee continues to work after the expiration of an employment contract with the Court noting that the common law presumption predates the judicial "establishment of the 'employment-at-will' doctrine."). *See also* Jyotin Hamid, *But You Promised Me A Promotion: Are False Inducements Actionable in At-Will Employment*, N.Y. ST. B.A.J., Oct. 2008, at 11-12.

31. Gary T. Marx, *Measuring Everything That Moves: The New Surveillance at Work*, *in* DEVIANCE IN THE WORKPLACE 165, 168 (Ida Harper Simpson et al. eds., 1999); *see also* Dobson & Fisher, *The Panopticon's Changing Geography*, 97 GEOGRAPHICAL REV. No. 3 (July 2007).

32. Marx, *supra* note 31, at 166-67.

33. *See, e.g.*, Ellen Perlman, *Where Are They Now?*, GOVERNING, Oct. 2005, *available at* http://www.governing.com/archive/2005/oct/gps.txt (discussing how states and localities are using GPS to track moving targets such as sex offenders and criminals, as well as their own law enforcement officers for safety purposes); Ellen Perlman, *Chip on Your Shoulder*, GOVERNING, Sept. 2005, *available at* http://www.governing.com/archive/2005/sep/rfid.txt (describing the advent of RFID technology, which was created for military purposes, in schools and office identification badges); Adam Geller, *New Uses of GPS Boost Productivity but Rankle Employees*, SEATTLE POST-

Unlike the Panopticon and Taylorism, however, contemporary technologies expand employment transparency beyond the workplace, thereby enabling employers to monitor employees even while not at work and propelling their reach into an employee's private life. Certain modern technologies, such as DNA testing, biometrics, and microchip implants, even penetrate employees' bodies.[34] Furthermore, unlike other forms of employment surveillance technologies, newer computer-based technologies automatically accumulate and store information without human judgment or discretion.

This article begins by reviewing the evolution of laws regulating genetic testing and discrimination in employment. Unlike other emerging technologies analyzed here, there has been significant analysis and foresight regarding the implications of genetic testing in employment. We first examine New York's regulatory scheme and then discuss the provisions of the 2008 federal legislation that establishes national standards in the area of genetic information and discrimination in the workplace.

A. LAW AND POLICY REGARDING GENETIC TESTING

Mandatory genetic testing refers to an employer's requirement that an individual submit to genetic and chromosomal testing for the purpose of determining the existence of genetic variations that demonstrate predispositions to disease or disability.[35] Genetic discrimination refers to an adverse employment or health benefits decision that is premised on genetic testing and genetic information of an individual.[36] New York's

INTELLIGENCER, Jan. 10, 2005, *available at* http://seattlepi.nwsource.com/business/207150_trackingworkers10.html (discussing the increase in use of GPS by employers for delivery or garbage trucks); Brandon Bain, *Suffolk's Spy in the Sky*, NEWSDAY (N.Y.), Mar. 31, 2006, at A3 (discussing plans for using GPS to track sex offenders, repeat drunk drivers, spousal abusers and drug dealers); Brandon Bain, *Tough to Track Abusers*, NEWSDAY (N.Y.), Apr. 10, 2006 (noting that the use of GPS to track sex offenders on Long Island is gaining support); Celeste Hadrick, *GPS Phones Will Home in on Homes*, NEWSDAY (N.Y.), Apr. 20, 2006 (providing an example of local governments monitoring their employees through cell phones with GPS chips). The United Kingdom's consideration of a plan for implanting prisoners with RFID microchips reinforces the relevance of the analogy to Bentham's Panopticon. *See* Iain Thomson, *UK Considers RFID Tags for Prisoners*, VNUNET.COM, Jan. 14, 2008, *available at* http://www.vnunet.com/vnunet/news/2207145/government-considers-rfid-tags.

34. An Ohio surveillance company was the first American company to announce that it commenced implanting RFID microchips in employees. Jonathan Sidener, *Implant ID Chips Called Big Advance, Big Brother*, SAN DIEGO UNION-TRIB., Mar. 12, 2006, at A1.

35. JEROO S. KOTVAL, N.Y. STATE LEGISLATIVE COMM'N ON SCI. & TECH., DNA-BASED TESTS: POLICY IMPLICATIONS FOR NEW YORK STATE, LCST Report No. 94-1, at 6, 14 (1994).

36. *Id.* at 13.

legislation governing genetic testing functions as a valuable model of proactive public policy aimed at balancing the respective interests of employers and employees regarding new technologies in employment.

On September 27, 1994, the New York State Legislative Commission on Science and Technology, chaired by Assemblyman Ronald J. Canestrari, issued a report prepared by scientist Dr. Jeroo S. Kotval regarding the implications of genetic testing.[37] The report examined the positive aspects of genetic testing, such as prospective assistance in combating disease,[38] as well as the foreseeable adverse consequences, including the potential for discrimination in employment and discrimination in the availability of health insurance.[39] By establishing a scientific, legal, and policy framework for evaluating genetic testing, the report facilitated the New York State Legislature's subsequent enactment of remedial legislation governing genetic testing in New York.[40]

In 1996, the Legislature amended the New York State Human Rights Law to ban employment discrimination based on an individual's genetic predisposition and to substantially limit the ability of employers to conduct genetic testing on employees or applicants.[41] The 1996 amendments codified the Legislature's conclusion that regulation was needed due to the potential danger that employers could use genetic testing as a means of controlling health insurance costs and "the possibility that even otherwise healthy individuals will be labeled genetically 'defective' and will form a growing 'genetic underclass' of society."[42] The legislation also reflected an important public policy determination that employee genetic privacy outweighed an employer's interest in potential savings on health care costs by denying employment to those individuals who may become ill due to a genetic predisposition.[43] As the Ninth Circuit has recognized, "[o]ne can think of few subject areas more personal and more likely to implicate privacy interests than that of one's health or genetic make-up."[44]

37. *Id.* at i.

38. *Id.* at 11-12.

39. *Id.* at 13-15.

40. *See id.* at i; N.Y. EXEC. LAW § 296(19)(a)-(d) (McKinney Supp. 2008).

41. *Id.* at §§ 296(1)(a), (19)(a)(1).

42. Act of Sept. 23, 1996, ch. 204, § 1, 1996 N.Y. Laws 343, 343 (McKinney).

43. *Id.* at 343-44.

44. Norman-Bloodsaw v. Lawrence Berkeley Lab., 135 F.3d 1260, 1269 (9th Cir. 1998) (citing Doe v. City of New York, 15 F.3d 264, 267 (2d Cir. 1994)). *See also* State v. Morel, 676 A.2d 1347, 1356 (R.I. 1996) (noting the legitimate privacy concerns that arise from the potential misuse of genetic information).

The New York State Legislature has remained proactive in the field of genetic testing and discrimination. In 2005, the New York State Human Rights Law was further amended to expand the statute's scope of protections against genetic discrimination.[45] Specifically, the amendment broadened the statutory ban on discrimination to include discrimination based on either test results or employer inferences resulting from personal or family information associated with a statistically significant increased risk of future diseases or disabilities.[46] The Legislature also refined the statute's technical language by deleting the phrases "genetic anomaly," "genetic predisposition," and "carrier," and replacing them with the phrase "predisposing genetic characteristic."[47]

Pursuant to New York Executive Law section 296(19)(a)(1), employers and other entities are prohibited from soliciting, requiring or administering a genetic test as a condition of employment or pre-employment application.[48] As part of the 2005 amendments, the Legislature clarified the definition of the phrase "genetic test" to mean: "a test for determining the presence or absence of an inherited genetic characteristic in an individual, including tests of nucleic acids such as DNA, RNA and mitochondrial DNA, chromosomes or proteins in order to identify a predisposing genetic characteristic."[49]

There are a number of exceptions to the general New York prohibition against genetic testing in employment. For example, an employer can require a specific genetic test if the test is "directly related to the occupational environment," such that a genetic anomaly could increase the risk of disease due to the surroundings.[50] In addition, genetic testing in New York is permissible when requested by an employee, with specific informed consent, for the purposes of: a workers' compensation claim, civil litigation, or to learn of the

45. Act of Aug. 29, 2005, ch. 75, 2005 N.Y. Sess. Laws 702, 702-03 (McKinney).

46. Memorandum in Support, Act of Aug. 29, 2005, ch. 75, 2005 N.Y. Sess. Laws 1984, 1984 (McKinney).

47. Act of Aug. 29, 2005, ch. 75, 2005 N.Y. Sess. Laws 702, 702-03 (McKinney). Under the amendment, "predisposing genetic characteristics" are defined as:

> [A]ny inherited gene or chromosome, or alteration thereof, and determined by a genetic test or inferred from information derived from an individual or family member that is scientifically or medically believed to predispose an individual or the offspring of that individual to a disease or disability, or to be associated with a statistically significant increased risk of development of a physical or mental disease or disability.

Id. at 702.

48. N.Y. EXEC. LAW § 296(19)(a)(1) (McKinney Supp. 2008).

49. *Id.* § 292(21-b).

50. *Id.* § 296(19)(b).

employee's susceptibility to workplace environmental hazards.[51] New advances in the application of DNA testing can provide important, if not dispositive, evidence to resolve the ultimate issue in toxic and workers compensation litigation: whether an individual was injured as a result of exposure to a particular chemical substance.[52]

In addition to establishing legal restrictions on genetic testing and discrimination in employment, New York has established a comprehensive legislative scheme within its Civil Rights Law that mandates written informed consent be obtained prior to any form of genetic testing for predisposition to disease.[53] Moreover, the law provides for specific confidentiality requirements and imposes civil and criminal penalties for statutory violations.[54]

Although New York law prohibits genetic testing in employment to determine genetic predisposition to disease and also prohibits the disclosure of genetic testing results to employers,[55] a significant exception exists in New York's genetic testing regulatory scheme. The present New York definition of "genetic test" is limited to tests for a "predisposing genetic characteristic" that correlates with an increased risk in the development of a disease or disability.[56] Based upon the statutory definition of "genetic test" it is improbable that an employer mandate for biological samples from employees for use in obtaining DNA identification information would be found to violate Executive Law section 296(19).

However, in light of the growing use of biometrics and other tracking technologies in employment, it may only be a matter of time before employers begin demanding DNA tests for the purpose of establishing genetic identification markers to aid in workplace security. In fact, MIT Professor Marx warned in 1998 that DNA fingerprinting might eventually become the most prominent means of identification.[57]

On both the federal and state level, laws have been enacted

51. *Id.* § 296(19)(c)-(d).

52. *See* Mark Hansen, *DNA Poised to Show Its Civil Side*, 94 ABA JOURNAL 18, 18-19 (Mar. 2008) (discussing the potential benefits and legal issues relating to the use of such testing in toxic tort and workers compensation litigation).

53. N.Y. CIV. RIGHTS LAW § 79-*l*(2)(a)-(b) (McKinney Supp. 2008).

54. *Id.* § 79-*l*(3).

55. N.Y. EXEC. LAW §§ 296(19)(a), 995-d(1) (McKinney Supp. 2008).

56. *See id.* § 296(19)(a)(1) (prohibiting the use of a genetic test "from which a predisposing genetic characteristic can be inferred"); N.Y. EXEC. LAW §292(21-a), (21-b) (McKinney Supp. 2008).

57. Gary T. Marx, *DNA 'Fingerprints' May One Day Be Our National ID Card*, WALL ST. J., Apr. 20, 1989, *available at* http://web.mit.edu/gtmarx/www/dna.html.

mandating forensic DNA testing for identification purposes.[58] These DNA-indexing statutes require that state and local officials extract biological samples from convicted criminals to establish genetic markers that are then entered in a DNA index or database maintained by federal and state entities.[59] This information can then be utilized by law enforcement to help identify perpetrators of other crimes.[60] These laws do not mandate nor prohibit employers from establishing employment-related DNA identification databases utilizing compelled or passive employee samples.

Like New York, many other states have proposed and enacted laws limiting the use of genetic information and testing, in particular, by placing similar prohibitions against discrimination based on an individual's genetic information.[61] In Washington, the state's statutory

58. However, most of these DNA identification laws apply only to felons. *See, e.g.*, Violent Crime Control & Law Enforcement Act of 1994 § 210304(a), 42 U.S.C. § 14132(a) (2001) (creating the Combined DNA Indexing System ("CODIS"), an FBI database containing DNA from anyone convicted of a federal felony); Idaho DNA Database Act of 1996, IDAHO CODE ANN. § 19-5501 to 19-5518 (2004) (requiring any person convicted of one of over sixty "serious crimes" to provide the Idaho State Police with a DNA sample, which is put into a CODIS-like database); N.Y. EXEC. LAW § 995-c(3) (McKinney 1996) (requiring offenders convicted of certain felonies to give blood for DNA analysis, the results of which are kept in an identification index); OR. REV. STAT. § 137.076 (West 2007) (requires persons convicted of murder, a sexual offense, or conspiracy or attempt to commit a sexual offense to submit a blood sample to the Oregon Department of Corrections ("DOC"), and requires the DOC to put the sample in a DNA data bank); VA. CODE ANN. § 19.2-310.2 (2008) (providing that all incarcerated felons shall provide the Commonwealth with a blood sample for a DNA bank, and authorizing the release of DNA information to federal, state and local law-enforcement officers upon request made in furtherance of an official criminal investigation).

59. *See, e.g.*, § 995-c(3).

60. According to the FBI, the CODIS DNA database has "produced over $76,100 hits assisting in more than 76,200 investigations." Federal Bureau of Investigation, *COIDS – NDIS Statistics* (2008), http://www.fbi.gov/hq/lab/codis/clickmap.htm. (last visited Dec. 28, 2008).

61. *See, e.g.*, ARIZ. REV. STAT. ANN. § 41-1463(B)(3) (2002); Genetic Information in the Workplace Act, ARK. CODE ANN. §§ 11-5-403 (2002); CAL. GOV'T CODE §§ 12926, 12940(e)-(f) (West 2005); CONN. GEN. STAT. ANN. § 46a–60(a)(11) (West 2004); DEL. CODE ANN. tit. 19, §§ 710, 711(e) (West 2006); 410 ILL. COMP. STAT. ANN. 513/25 to /30 (West 2005); KAN. STAT. ANN. §§ 44-1002(m), 1009(a)(9) (2000); LA. REV. STAT. ANN. §§ 22:213.7, 23:368 (1998 & Supp. 2008); MD. CODE ANN., PUB. GEN. LAWS art. 49B, § 16(a)(3) (LexisNexis 2003); MASS. GEN. LAWS ANN. ch. 151B, §§ 1(22), 4(19) (West 2004 & Supp. 2007); MICH. COMP. LAWS ANN. §§ 37.1201-.1202 (West 2001 & Supp. 2008); MINN. STAT. ANN. § 181.974 (West 2006); MO. ANN. STAT. §§ 375.1300, 1306 (West 2002 & Supp. 2008); NEV. REV. STAT. ANN. § 613.345 (LexisNexis 2006); N.H. REV. STAT. ANN. § 141-H:3 (2005); N.J. STAT. ANN. §§ 10:5-5, -12(a) (West 2002); N.C. GEN. STAT. ANN. § 95-28.1A (West 2005); Genetic Nondiscrimination in Employment Act, OKLA. STAT. ANN. tit. 36, § 3614.2 (West 2006); OR. REV. STAT. § 659A.303 (2005); R.I. GEN. LAWS § 28-6.7-1 (2003); S.D. CODIFIED LAWS § 60-2-20 to -21 (2004); TEX. LAB. CODE ANN. § 21.402 (Vernon 2006); UTAH CODE ANN. § 26-45-103 (Supp. 2007); VT. STAT. ANN. tit. 18, § 9333 (2007); VA. CODE ANN. § 40.1-28.7:1 (2002 & Supp. 2008); WASH. REV. CODE ANN. § 49.44.180 (West 2008); WIS. STAT. ANN. §§ 111.32(7m), 372. In addition, the EEOC has interpreted the Americans with Disabilities Act ("ADA") to prohibit discrimination based on an individual's

provisions governing genetic privacy were the product of a Genetics Task Force ("G.T.F.") convened by the Washington Board of Health to evaluate state policies regarding genetic information, including issues relating to privacy, civil rights, research, and development.[62] Following a study by a Georgia legislative committee, the Georgia House of Representatives introduced the Biometric Information Protection Act ("BIPA") in February 2007 which would, *inter alia*, prohibit employers from utilizing information derived from genetic testing.[63] Although the scope of these state legislative initiatives varies widely, they are indicative of the national consensus that has developed in response to the results of the genome project: while genetic technology has great promise to improve society in multiple ways, employment discrimination toward an individual based on genetic composition or participation in genetic testing should not be lawful.

This national consensus has culminated in the enactment of the federal Genetic Information Nondiscrimination Act of 2008[64] ("GINA"). GINA represents a significant step forward for U.S. law and policy by establishing national standards in the areas of genetic testing and discrimination in employment following years of congressional study, analysis, and debate, as well as, significant opposition. For example, the U.S. Chamber of Commerce in 2004 opposed a similar proposal on the grounds that there was insufficient evidence of genetic discrimination in the country to warrant federal remedial legislation.[65] GINA establishes

genetic profile on the grounds that such an individual is a person regarded as disabled under the ADA. *See* Americans with Disabilities Act, 42 U.S.C. § 12102(2)(C) (2000) ("The term 'disability' means, with respect to an individual – (C) being regarded as having such an impairment."). Section 4 of the Americans with Disabilities Act Amendments Act of 2008 has modified the statutory definition of disability under § 12102(3) to provide that the requirement of "being regarded as having such an impairment" can be established by demonstrating that an individual has been subject to an action prohibited by the ADA "because of an actual or perceived physical or mental impairment whether or not the impairment limits or is perceived to limit a major life activity." ADA Amendments Act of 2008, S. 3406, 110th Cong. § 4(a) (2008). However, the substantive relevancy of the ADA to genetic discrimination has been substantially diminished by the enactment of the Genetic Information Nondiscrimination Act of 2008.

62. *See* Linda Lake, *Introduction* to WASH. STATE BD. OF HEALTH GENETICS TASK FORCE, WASH. STATE BD. OF HEALTH, A REPORT TO THE WASHINGTON STATE LEGISLATURE: GENETIC PRIVACY, DISCRIMINATION, AND RESEARCH IN WASHINGTON STATE (2002), *available at* http://www.sboh.wa.gov/Goals/Past/Genetics/documents/GTFReportMaster.pdf.

63. H.R. 276, 149th Gen. Assem. Reg. Sess. At § 10-12A-6(1) (Ga. 2007), *available at* http://www.legis.ga.gov/legis/2007_08/search/hb276.htm (follow "PDF Version" hyperlink).

64. Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233, 122 Stat. 905 (codified at 42 U.S.C. § 2000ff-8).

65. *Genetic Non-Discrimination: Examining the Implications for Workers and Employers: Hearing Before the H. Subcomm. on Employer-Employee Relations of the H. Comm. on Educ. & the Workforce*, 108th Cong. (2004) (statement of Lawrence Z. Lorber, Partner, Proskauer Rose LLP on

strict federal limitations on the collection, monitoring, and use of genetic information by employers, employment agencies, labor unions, and training programs.[66] However, the GINA provisions applicable to the workplace do not become effective until October 2009, eighteen months after the statute's enactment.[67]

In its findings, Congress acknowledged that there are many medical benefits associated with genetic research, including providing an opportunity for earlier detection and treatment for genetically based diseases.[68] At the same time, Congress referred to the dangers inherent in genetic testing citing twentieth century American laws, inspired by the eugenics movement, which mandated the sterilization of people with purported genetic defects,[69] as well as more recent attempts to mandate testing of sickle cell anemia in African-Americans.[70]

Congress specified that GINA is intended to establish a uniform standard of substantive rights which should not be construed as preempting or placing limitations on other state and federal laws that provide equal or greater protections.[71] A central tenet of the legislation is to encourage individuals to take advantages of the benefits of genetic technology without having to fear that participation in genetic testing and studies will endanger job opportunities or health benefits.[72] One of

behalf of the U.S. Chamber of Commerce), *available at* http://www.uschamber.com/issues/testimony/2004/040722lorbergenetics.htm (follow "View the Testimony" hyperlink).

66. *See* §§ 202(b)-(c), 203(b)-(c), 204(b)-(c), 205(b)-(c).

67. § 213.

68. § 2(1).

69. The scope of the original American legal acceptance of the tenets of eugenics is highlighted by Justice Holmes' rejection of due process and equal protection challenges to Virginia's sterilization law. Buck v. Bell, 274 U.S. 200, 207 (1927). In his majority opinion, Justice Holmes starkly articulated the rationale for the Court's conclusion that a State mandatory sterilization program was constitutional:

> It would be strange if it could not call upon those who already sap the strength of the State for these lesser sacrifices, often not felt to be such by those concerned, in order to prevent our being swamped with incompetence. It is better for all the world, if instead of waiting to execute degenerate offspring for crime, or to let them starve for their imbecility, society can prevent those who are manifestly unfit from continuing their kind. The principle that sustains compulsory vaccination is broad enough to cover cutting the Fallopian tubes. Three generations of imbeciles are enough.

Id. at 207 (citation omitted). The subsequent Nazi ideological embrace of eugenics to justify its crimes against humanity has resulted in a systematic repudiation of eugenic theory in the United States. *See generally* André N. Sofair & Lauris C. Kaldjian, *Eugenic Sterilization and a Qualified Nazi Analogy: The United States and Germany, 1930-1945*, 132 ANNALS OF INTERNAL MED. 312 (2000).

70. § 2(3).

71. § 209(a)(1).

72. § 2(4)-(5).

the discoveries stemming from genetic research, cited in GINA's legislative history, is the correlative link between an elevated risk of breast and ovarian cancer and two genetic mutations.[73]

Modeled generally after the substantive anti-discrimination provisions of Title VII of the Civil Rights Act of 1964[74] ("Title VII"), GINA makes it an unlawful employment practice for employers, employment agencies, labor unions, and training programs to engage in discrimination based on genetic information.[75] In contrast to Title VII's prohibition against employment discrimination against "any individual," GINA prohibits discrimination by employers against an "employee," defined as including job applicants.[76] The purpose for this variation is unclear from the legislative history; however, the use of the term "employee" by the GINA drafters may have substantive importance when the scope of the statute's protections is subject to judicial interpretation.

The term "genetic information" is defined broadly by GINA to mean an "individual's genetic tests, . . . the genetic tests of family members of such individual, and . . . the manifestation of a disease or disorder in family members of such individual."[77] The statutory definition also includes an individual's receipt of genetic services and participation in genetic research, but the definition excludes information about an individual's sex or age.[78] GINA does not, however, prohibit "the use, acquisition, or disclosure of medical information that is not genetic information about a manifested disease, disorder, or pathological condition of an employee or member, including a manifested disease, disorder, or pathological condition that has or may have a genetic basis."[79]

Consistent with New York's statutory scheme, GINA does not explicitly prohibit employers from utilizing DNA testing or results for employee identification purposes.[80] The term "genetic test" in GINA is limited to the "analysis of human DNA, RNA, chromosomes, proteins,

73. *See* Anita Silvers & Michael Ashley Stein, *An Equality Paradigm for Preventing Genetic Discrimination*, 55 VAND. L. REV. 1341, 1352 (2002) (citing Julian Borger, *Health Warning as DNA Screening Takes Hold, Americans Find it Can Leave Them Unemployed and Uninsured: Who's Testing Our Genes – and Why?*, GUARDIAN (London), Sept. 19, 2000, at 15.

74. 42 U.S.C. §§ 1971, 1975a-1975d, 2000a-2000h-6 (2000).

75. *See* §§ 202(b)-(c), 203(b)-(c), 204(b)-(c), 205(b)-(c).

76. *See* § 201(2)(A); 42 U.S.C. § 2000e(f).

77. § 201(4)(A).

78. § 201(4)(B).

79. § 210.

80. § 202(b).

or metabolites, that detects genotypes, mutations, or chromosomal changes."[81] Testing for DNA sequences for identification purposes are not included in GINA's definition of genetic testing.[82]

In addition to prohibiting employment discrimination based on genetic information, GINA also restricts employers generally from "request[ing], requir[ing], or purchas[ing] genetic information with respect to an employee or a family member of the employee."[83] Significantly, GINA defines "family member" broadly to include any dependent or other individual within the fourth degree of consanguinity.[84]

There are multiple exceptions to the general rule against the acquisition of genetic information which will inevitably be a rich source for future litigation on par with the scope of litigation stemming from the original statutory definition of the term "disability" under the Americans with Disabilities Act of 1990[85] ("ADA").[86]

The most notable exception to the restriction on the acquisition of genetic information is the exclusion "where an employer inadvertently requests or requires" genetic information.[87] This exception stems from a congressional concern that stray remarks about genetic information around a water cooler should not be deemed unlawful. In responding to this concern, however, Congress has codified an exception that may be described fairly as an oxymoron: an "inadvertent" requirement that an employee provide genetic information.[88] Under this exception, employers, unions and other entities can require genetic information, but still retain a statutory defense that the demand is protected by GINA because it was inadvertent.[89]

Other statutory exceptions to the restriction on acquisition of

81. § 201(7).

82. Reflecting the broader scope of European privacy protections, the European Court of Human Rights recently concluded that the United Kingdom violated Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms by retaining DNA profiles and cellular samples of individuals acquitted of criminal conduct. *See* S. & Marper v. the United Kingdom, [2008] ECHR 1581, *available at* http://www.bailii.org/eu/cases/ECHR/2008/1581.html.

83. § 202(b).

84. § 201(3).

85. 42 U.S.C. §12101.

86. One of the primary purposes of the Americans with Disabilities Act Amendments Act of 2008 was to overturn U.S. Supreme Court decisions that judicially imposed a narrow construction on the scope of protections Congress intended to be afforded by the ADA. ADA Amendments Act of 2008, S. 3406, 110th Cong. § 2 (2008); *see* Sutton v. United Air Lines, Inc., 527 U.S. 471 (1999); Toyota Motor Mfg., Ky., Inc. v. Williams, 534 U.S. 184 (2002).

87. § 202(b)(1).

88. *See* § 202(b)(1).

89. *See* §§ 202(b)(1), 203(b)(1), 204(b)(1), 205(b)(1).

genetic information include: a) where an employee has provided explicit and voluntary consent in conjunction with health or genetic services offered by the employer as part of a wellness program; b) where family medical history is needed to comply with the certification provisions of the Family and Medical Leave Act; c) where the employer purchases documents containing family medical history that are commercially and publicly available such as newspapers, periodicals, and books (this exception is inapplicable to medical databases or court records); and d) where the information is sought as part of the employer's genetic monitoring of the biological effects of toxic substances in the workplace, so long as the employer meets various statutory preconditions including providing written notice of the genetic monitoring to the employee and provides the individual results to the employee.[90]

In situations where an employer is permitted under GINA to possess genetic information, the employer is required to maintain the information as a confidential record under the ADA.[91] Genetic information in the possession of an employer can not be disclosed unless such disclosure is authorized under one of the six statutory grounds set forth in GINA.[92]

The employment discrimination provisions in GINA are enforceable under Title VII procedures.[93] However, as part of the compromise that resulted in its enactment, GINA does not establish a cause of action for disparate impact with respect to genetic information and discrimination.[94] But GINA does not completely ignore the possibility of disparate impacts, as it mandate the establishment of a Genetic Nondiscrimination Study Commission, six years after GINA's enactment, "to review the developing science of genetics and to make recommendations to Congress regarding whether to provide a disparate impact cause of action" with respect to genetic information.[95]

Finally, this discussion of GINA's substantive and procedural provisions applicable to employment should not overshadow the potential relevance of another federal statute, the National Labor Relations Act[96] ("NLRA"), as it relates to the subject to genetic testing in employment. Whether genetic testing, in any form, constitutes a

90. § 202(b)(2)-(5).
91. § 206(a).
92. § 206(b).
93. § 207(a)(1).
94. § 208(a).
95. § 208(b).
96. 29 U.S.C. §§ 151-169 (2000).

mandatory subject of bargaining under the NLRA is yet to be determined.[97] However, it is possible, that the National Labor Relations Board may rely on prior precedent regarding the negotiability of drug and alcohol testing to conclude that genetic testing for predisposition to illness or identification constitutes a mandatory subject of bargaining.[98]

B. LAW AND POLICY REGARDING GPS TECHNOLOGY

Although Congress and many states have studied and enacted legislation regulating genetic testing in employment, the public policy issues relating to GPS tracking in employment remain largely unexplored.[99] GPS devices provide nearly precise location information of objects or individuals on a real-time basis by triangulating satellite signals.[100] The most widely recognized GPS technology is the navigational accessory available in many newer vehicles.[101] GPS technology can also be found in portable objects such as cell phones, laptops, BlackBerrys, and PDAs.[102]

In light of the growing ubiquity of GPS technology, University of Kansas Professor Jerome E. Dobson has articulated concerns regarding the prospective abuse of the technology by those in power. Professor Dobson and one of his colleagues have labeled the potentially abusive use of location technology as "geoslavery."[103] Moreover, the increasingly narrow line separating work and pleasure provides "the strongest basis for imposing limits on an employer's right to peer into the private lives of its workers," according to Professor Michael Selmi.[104]

97. *See generally* 29 U.S.C. § 158(d) (defining the obligation to collectively bargain under the NLRA).

98. *See* Johnson-Bateman Co., 295 N.L.R.B. 180, 182 (1989).

99. In contrast, several states have enacted various criminal statutes and consumer protections regarding the use of GPS technology. *See, e.g.*, CAL. CIV. CODE § 1936(o)(1)(B)(3) (West Supp. 2008); TEX. PENAL CODE ANN. § 16.06 (Vernon 2003). *See also* Elizabeth C. Yen, *Rent a Car, Rent a Spy*, 14 BUS. L. TODAY 6, Aug. 2005, *available at* http://www.abanet.org/buslaw/blt/2005-07-08/yen.shtml (discussing legislation in New York, California, and Connecticut that restricts the car rental industry's ability to use GPS information).

100. April A. Otterberg, *GPS Tracking Technology: The Case for Revisiting* Knotts *and Shifting the Supreme Court's Theory of Public Space Under the Fourth Amendment*, 46 B.C. L. REV. 661, 663, 665 (2005).

101. Kristen E. Edmundson, *Global Positioning System Implants: Must Consumer Privacy Be Lost in Order for People to Be Found?*, 38 IND. L. REV. 207, 210 (2005).

102. *See* Otterberg, *supra* note 100, at 666-68; Edmundson, *supra* note 101, at 210.

103. Jerome E. Dobson & Peter F. Fisher, *Geoslavery*, IEEE TECH. & SOC'Y MAG., Spring 2003, at 47, 47-48.

104. Selmi, *supra* note 28, at 1046.

Most case law regarding the use of GPS technology has focused on whether a warrant is required under federal or state constitutions before a GPS device can be used by law enforcement to track vehicles.[105] Based on existing Fourth Amendment precedent regarding the use of beepers to monitor vehicular movement, it is unlikely that a majority of the current U.S. Supreme Court would conclude that law enforcement's warrantless use of GPS technology to track vehicles in a criminal investigation violates the Fourth Amendment.[106]

However, a different constitutional holding is possible when the same technology is used to monitor individuals or objects within an individual's home.[107] In addition, the scope in which the technology is utilized by law enforcement may result in a Fourth Amendment violation. For example, in *United States v. Garcia*,[108] the Seventh Circuit concluded that police placement of a GPS device on a car constituted neither a search nor seizure and thereby did not invoke the Fourth Amendment.[109] In *dicta*, Judge Posner acknowledged that the propriety of law enforcement's use of GPS technology on a single suspect is a separate and discrete issue from the future possibility that law enforcement may utilize similar technology for mass indiscriminate surveillance.[110] It remains to be seen whether this distinction under the Fourth Amendment between targeted versus indiscriminate use of the

105. *See, e.g.*, United States v. Dubrosky, 581 F.2d 208, 211-12 (9th Cir. 1978) (upholding the use of a beeper tracking device, likening it to an enhancement of the fives senses, the use of which does not require a warrant); United States v. Bruneau, 594 F.2d 1190, 1193-94 (8th Cir. 1979) (holding the use of a transponder in an airplane does not constitute a search requiring a warrant); United States v. Lewis, 621 F.2d 1382, 1387-88 (5th Cir. 1980) (a warrant is unnecessary because "the Fourth Amendment does not prohibit the placement of a beeper in a drum or box before the defendant takes possession.").

106. *See, e.g.*, United States v. Knotts, 460 U.S. 276, 284-85 (1983) (holding 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). The Supreme Court emphasized that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." *Id.* at 281.

107. *See, e.g.*, United States v. Karo, 468 U.S. 705, 714-16 (1984) (holding that use of a beeper to determine whether an object was inside a home was subject to the warrant requirement by applying the core Fourth Amendment principle that warrantless search and seizure inside a home is presumptively unreasonable absent an exigent circumstance); Kyllo v. United States, 533 U.S. 27, 29, 40 (2001) (holding that use of a thermal-imaging device, without a warrant, to detect high-density lamps used to grow marijuana inside a home violated the Fourth Amendment). The Court in *Kyllo* noted: "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." *Id.* at 40.

108. 474 F.3d 994 (7th Cir. 2007).

109. *Id.* at 996-98.

110. *Id.* at 998.

technology will be considered in future cases examining the implementation and use of GPS technology.

State constitutional provisions may provide the basis for greater constitutional limitations on the use of GPS technology. The highest courts of Oregon and Washington both held that their respective state constitutions require the police to obtain a warrant before utilizing tracking technologies such as GPS.[111] Nevertheless, the Oregon Supreme Court has ruled that the police placing a transmitter on a public employer's vehicle without a warrant did not violate an employee's right to privacy under the Oregon Constitution.[112]

In *People v. Weaver*,[113] an intermediate appellate court ruled that the New York State Constitution did not require the police to obtain a warrant before attaching a GPS device to a vehicle's bumper, located on a public street, because individuals have a substantially diminished expectation of privacy while on a public roadway.[114] In reaching its holding, the New York court distinguished Oregon and Washington precedent by emphasizing that those decisions relied on the disproportionate intrusive nature of the technology rather than whether the individual had a reasonable expectation of privacy.[115] In the dissent, Justice Stein rejected the rationale that GPS-based surveillance is equivalent to monitoring through human observation or supervision.[116] In Justice Stein's view, "the enhancement of our ability to observe by the use of technological advances compels us to view differently the circumstances in which an expectation of privacy is reasonable."[117]

The New Jersey Supreme Court has upheld the issuance of a warrant based on probable cause for the installation of a GPS device without reaching the question of whether such a warrant was mandatory under the New Jersey Constitution.[118] In the same year, New Hampshire

111. State v. Campbell, 759 P.2d 1040, 1045, 1049 (Or. 1988) (interpreting the Oregon Constitution to prohibit the police's warrantless use of a radio transmitter to locate a private vehicle and rejecting the Supreme Court's rationale in *Knotts*, as the transmitter was determined to be a location finder rather than a mere extension of police visual tracking); State v. Jackson, 76 P.3d 217, 230-31 (Wash. 2003) (en banc) (holding that a warrant was required under the Washington Constitution before the police could attach a GPS device to a vehicle).

112. State v. Meredith, 96 P.3d 342, 346 (Or. 2004) (distinguishing *Campbell*, 759 P.2d at 1049).

113. 860 N.Y.S.2d 223 (N.Y. App. Div. 2008), *appeal granted* 10 N.Y.3d 966 (2008).

114. *Id.* at 225-26.

115. *Id.* at 226 n.2.

116. *Id.* at 228.

117. *Id.*

118. *See* State v. Scott, No. 02-02-00121-I, 2006 WL 2640221, at *8, 10 (N.J. App. Div. Sept. 15, 2006).

enacted a law prohibiting the police from utilizing GPS as a means to determine the ownership or occupancy of a motor vehicle.[119]

The relatively slow introduction of GPS technology in employment contexts may explain the lack of governmental attention to the subject. According to the 2005 Electronic Monitoring and Surveillance Survey from the American Management Association and the ePolicy Institute, five percent of employers surveyed used GPS technology to track employees through cell phones and eight percent utilized it to track employer vehicles.[120] However, given the aggressive marketing of location-based services by telecommunications companies, it is reasonable to expect a sharp increase in the implementation of GPS technology in employment. For example, in March 2006, over 100 employers attended a GPS conference on Long Island sponsored by a company offering location based services.[121] Similarly, the New York City Fire Department has installed GPS technology in fire trucks and ambulances.[122]

In addition to utilizing GPS technology for property protection and employee monitoring, the technology is also being implemented by employers in some industries to protect workers' safety. For example, New York City has announced plans to implant GPS microchips in firefighters' gear to help track firefighters' whereabouts while inside unsafe and burning buildings.[123] The National Institute for Occupational Safety and Health has been studying GPS as a technological means of identifying unsafe outdoor work locations.[124] GPS microchips installed in most cell phones also have the potential to aid in the search for lost or abducted individuals.[125]

The introduction of GPS technology to monitor employees in real time represents a major step toward creating a technological Panopticon,

119. N.H. REV. STAT. ANN. § 236:130 (Supp. 2008).

120. AM. MGMT ASS'N & EPOLICY INST. RESEARCH, 2005 ELECTRONIC MONITORING & SURVEILLANCE SURVEY 2 (2005).

121. Brandon Bain, *Towns Eye Tech at GPS Summit*, NEWSDAY (N.Y.), Mar. 23, 2006, at A48.

122. Christopher Faherty, *Other Cities Race Ahead of New York on Fire Technology*, N.Y. SUN, Mar. 15, 2007, *available at* http://www.nysun.com/article/50501?page_no=1; Fire Rescue 1, *New York City to Install GPS Systems in All Fire and EMS Vehicles*, Apr. 26, 2006, http://www.firerescue1.com/technology/official-announcements/103609.

123. David Seifman, *FDNY Tracking Chip a Bravest New World*, N.Y. POST, Feb. 24, 2007, at 2.

124. Nat'l Inst. for Occupational Safety & Health, Ctr. for Disease Control, *NIOSH Prototype GPS Monitor Promises Faster, Surer Way to Identify Exposures*, July 18, 2003, http://www.cdc.gov/niosh/updates/gpsexpo.html.

125. Terri Sanginiti, *Cell Phone's GPS Leads Police to Abducted Mom*, NEWS J. (Del.), Mar. 22, 2007, at 1B.

and as Professor Richard Bales noted, constitutes "an important indicator of employer control."[126] Under the NLRA, however, employees have little control over use of their own personal technological devices during the workday.[127] The scope of employer dominance over the use of technology in the workplace was reinforced by a 2004 memorandum issued by the NLRB Division of Advice, which concluded that an employer's ban on employee use of personal communication devices, such as cell phones and pagers, during work time did not violate the NLRA.[128]

Professor Selmi has postulated that based on the continued viability of the at-will doctrine in the United States, it would be very difficult for an employee to successfully assert a legally-protected workplace privacy interest broad enough to restrict employer use of GPS technology.[129] Echoing the reasoning of former Chief Justice Rehnquist with respect to beeper devices in *United States v. Knotts*,[130] Professor Selmi expressed the view that the use of GPS technology to track vehicles or individuals constitutes only a more efficient means of visual monitoring.[131] Professor Selmi's reasoning conflicts with the Washington Supreme Court's recognition of the extraordinary intrusiveness of the fruits of this technology.[132] Unlike visual monitoring, GPS technology is computer-assisted, stores information in a database for long-term retrieval, can yield various reports that document real-time movement and speed of a vehicle or an individual, and does not require human supervisory control.[133]

Based on the recent introduction of GPS technology in employment, there are few employment decisions that include a

126. Posting of Richard Bales to Workplace Prof Blog, http://lawprofessors.typepad.com/laborprof_blog/2006/08/gps_tracking_of.html (Aug. 7, 2006).

127. *See* Banca Di Roma, Assoc. Gen. Counsel Advisory Memorandum, Case No. 13-CA-41283-1 (Nov. 26, 2004) *available at* http://www.nlrb.gov/research/memos/advice_memos/index.aspx (follow "Year:2004" drop-down menu; then follow "Banca Di Roma" PDF link).

128. *Id.*

129. Selmi, *supra* note 28, at 1042-45.

130. 460 U.S. 276 (1983).

131. *Compare* Selmi, *supra* note 28, at 1045, *with Knotts*, 460 U.S. at 282, 284 ("We have never equated police efficiency with unconstitutionality, and we decline to do so now.").

132. *Compare* Selmi, *supra* note 28, at 1045 (stating that GPS devices are little more than a substitute for visual monitoring and that the devices are more efficient does not give rise to a legitimate privacy interest), *with* State v. Jackson, 76 P.3d 217, 223-24 (Wash. 2003) (en banc) (discussing the differences in intrusion between visual surveillance and GPS devices and requiring a warrant for attachment of a GPS device to a citizen's vehicle).

133. Eva Marie Dowdell, *You Are Here! - Mapping the Boundaries of the Fourth Amendment with GPS Technology*, 32 RUTGERS COMPUTER & TECH. L.J. 109, 112, 116-17 (2005).

discussion of the technology. Most reported cases deal with challenges to disciplinary investigations and adverse actions based on employer use of GPS technology.[134]

In Missouri, a federal judge dismissed an employee's challenge to an employer's use of GPS in an employer-owned truck as part of a disciplinary investigation regarding theft.[135] Similarly, Oregon's Supreme Court rejected a public employee's privacy claim regarding the installation of a GPS device in a work vehicle.[136] In *Spinks v. Township of Clinton*,[137] a New Jersey court dismissed retaliation claims brought by police officers who charged that they were subjected to GPS surveillance as a result of earlier discrimination complaints.[138] In that case, GPS technology was used to establish that the police officers had falsified time records, which led to their resignations, guilty pleas, and in one case a conviction after a jury trial.[139]

In Connecticut, legal efforts to enjoin city officials from pursuing disciplinary charges against two employees based on evidence obtained through GPS devices secretly installed in municipal vehicles were unsuccessful.[140] In those cases, the plaintiffs contended that the city had violated their rights under a Connecticut statute that establishes certain limits on employer use of electronic surveillance devices.[141] In dismissing the lawsuits, the Connecticut court concluded that the state statute was inapplicable to electronic devices in employer vehicles and that the plaintiffs had failed to exhaust their contractual administrative

134. *See, e.g.*, Elgin v. St. Louis Coca-Cola Bottling Co., No. 4:05CV970-DJS, 2005 WL 3050633, at *1 (E.D. Mo. 2005) (involving allegations that the employer used GPS monitoring as a form of racial discrimination); State v. Meredith, 96 P.3d 342, 342-43 (Or. 2004) (admitting information obtained from GPS device employer placed on work truck to convict defendant of arson); Spinks v. Township of Clinton, 955 A.2d 304, 307 (N.J. Super. Ct. App. Div. 2008) (exemplifying the role of GPS in the discharge of patrol officers).

135. *Elgin*, 2005 WL 3050633, at *1.

136. *Meredith*, 96 P.3d at 342-43. Based on decisions interpreting the scope of the Fourth Amendment, it is questionable whether employee privacy claims challenging the use of GPS devices in employer-owned vehicles during work time will be successful. *See, e.g.*, *Knotts*, 460 U.S. at 281-82, 285; *but cf. Jackson*, 76 P.3d, 230-31 (holding that attachment of a GPS device to a vehicle without a warrant would be unconstitutional under Washington's state constitution).

137. No. HNT-L-342-03, 2006 WL 941973 (N.J. Super. Ct. Law Div. 2006), *aff'd*, 955 A.2d 298 (N.J. Super. Ct. App. Div. 2008).

138. *Id.* at *1, 10, 16.

139. *Id.* at *1-2.

140. Gerardi v. City of Bridgeport, No. CV084023011S, 2007 Conn. Super. LEXIS 3446 (Conn. Super. Ct. Dec. 31, 2007) (unreported); Vitka v. City of Bridgeport, No. CV0804022961S, 2007 Conn. Super. LEXIS 3486 (Conn. Super. Ct. Dec. 31, 2007) (unreported).

141. *Gerardi*, 2007 LEXIS 3446, at *1; *see Vitka*, LEXIS 3486, at *1; CONN. GEN. STAT. ANN. §§ 31-48b and 31-48d (West 1958).

remedies.[142]

The Tenth Circuit Court of Appeals affirmed the grant of summary judgment against a truck driver in his GPS-related duty of fair representation claim against the International Brotherhood of Teamsters ("IBT").[143] In *Hinkley v. Roadway Express, Inc.*,[144] the IBT had negotiated a collective bargaining agreement with the trucking company containing a provision that prohibited the use of computer tracking devices for disciplinary purposes.[145] Nevertheless, the company, after comparing the driver's recording of his deliveries and pick-ups with computerized location information emanating from the GPS device in the truck, fired the driver for making an unauthorized personal stop at a store.[146] In support of the driver's grievance the IBT argued that he should be reinstated with back wages because the company had used the GPS tracking information to discipline the driver in violation of the contract.[147] The IBT's contractual argument was successful to the extent that the tracking information was excluded from the grievance hearing.[148] However, the driver's termination was nevertheless upheld by the grievance board.[149] Thereafter, the driver commenced a federal action claiming that the IBT had allegedly violated its duty of fair representation.[150] The Tenth Circuit affirmed the dismissal of the duty of fair representation claim on the grounds that the IBT's representation of the driver was not arbitrary, discriminatory, or perfunctory.[151]

In 2006, a Massachusetts federal judge enjoined a union from going on strike, in violation of a no-strike contract provision, over disputes relating to the introduction of GPS technology to monitor employees.[152] Notably, the employer and the union in that case presented very different perspectives relating to the purpose of the GPS technology.[153] While the employer described the GPS technology as being a safety tool, the union

142. *Gerardi*, 2007 LEXIS 3446, at *20; *Vitka*, LEXIS 3486, at *20.

143. Hinkley v. Roadway Express, Inc., 2007 U.S. App. LEXIS 21938 (10th Cir. Sept. 13, 2007).

144. 2007 U.S. App. LEXIS 21938 (10th Cir. Sept. 13, 2007).

145. *Id.* at 14-15.

146. *Id.* at 15.

147. *Id.*

148. *Id.* at 16.

149. *Id.*

150. *Id.*

151. *Id.* at 17.

152. Kone, Inc. v. Local 4 Int'l Union of Elevator Constructors, No. 06-10093-DPW 2006 WL 2987042 at *12 (D. Mass. Sept. 27, 2006).

153. *Id.* at *3 n.2.

argued that it lacked any safety value.[154] A similar dispute over the benefits of GPS technology surfaced in New York City when an alliance of taxi drivers was unsuccessful in enjoining a municipal mandate that all licensed cabs install equipment containing GPS technology.[155]

By its intrusive nature, GPS technology can create the impression of surveillance in a way that may violate the NLRA because employees can reasonably believe that their employer can track them while participating in protected activities.[156] In addition, the real-time reports available via the technology can provide employers with important information that may aid in suppressing or retarding union-related activities or collective action protected under the NLRA. Meanwhile, although such actual surveillance would be unlawful, the establishment of a uniform system of employee tracking, combined with the complexity of the technology, may render it very difficult to demonstrate direct statutory violations under the NLRA. Furthermore, whether the NLRA imposes a statutory duty to bargain an employer's decision to implement GPS technology remains unresolved.

The IBT in the United States and the Canadian Union of Postal Workers ("CUPW") have negotiated contractual clauses limiting how employers can utilize the information obtained through GPS technology.[157] In addition, the union representing engineers and scientists employed by the State of Massachusetts negotiated an agreement regarding mandatory employee use of GPS-equipped cell phones.[158] Under the agreement, GPS devices must be on during all work hours but the device can be turned off during breaks and

154. *Id.*

155. Alexandre v. New York City Taxi & Limousine Comm'n, 2007 U.S. Dist. LEXIS 73642 (S.D.N.Y. Sept. 28, 2007).

156. The relevant standard regarding an employer creating the impression of surveillance was recently restated by the NLRB in *Ivy Steel & Wire, Inc.* 346 N.L.R.B. No. 41, at 404 (2006). "[T]he test for determining whether an employer has created an impression of surveillance is whether the employee would reasonably assume from the statement that their [sic] union activities had been placed under surveillance." Fred'k Wallace & Son, Inc., 331 N.L.R.B. 914, 914 (2000) (alteration in original) (quoting Flexsteel Indus., 311 N.L.R.B. 257, 257 (1993)).

157. The National Master UPS-Teamsters contract provides: "No employee shall be disciplined for exceeding personal time based on data received from the DIAD/IVIS or other information technology." National Master United Parcel Service Agreement, art. 37, § 1(d) (2002), *available at* http://www.browncafe.com/ups_national_master_agreement.html. The Canadian Post-CUPW contract provides: "At no time may such [watch and observation] systems be used as a means to evaluate the performance of employees and to gather evidence in support of disciplinary measures unless such disciplinary measures result from the commission of a criminal act." BIBBY, *supra* note 2, at 15 (alteration in original).

158. Settlement Agreement, Mass. Org. of State Eng'rs & Scientists v. Commonwealth, (Feb. 16, 2005) (on file with author).

lunches.[159] If the State inadvertently gathers data during breaks and lunches, such data would be destroyed.[160] The agreement also provides for employee training about the technology as well as union access to the data based on its role as collective bargaining representative.[161]

In 2007, a police union entered into an agreement with a New York public employer wherein the employer agreed "not to use GPS technology of any kind to initiate discipline against any police officer, although it may be used for all other lawful (including evidentiary) purposes."[162] By contrast, other collective bargaining agreements contain language granting employers blanket discretion to constantly upgrade technologies in the workplace.[163]

The potential for abuse stemming from the use of GPS technology strongly suggests the need for careful and probative legislative analysis regarding the public policy implications of the technology. Although employers traditionally have been granted wide latitude in implementing significant restrictions on employee freedom of movement during working hours,[164] the magnitude of the technology's potential intrusion into individual privacy warrants a review of the full policy implications.

The digital nature of the technology results in the perpetual gathering of location information without regard to time or place. The portability of the technology in cell phones and other devices can enable an employer to engage in or have access to computer-based real time location intelligence while an employee is at home, on break, or engaged in non-work related activities while off-duty. The public policy implications are particularly troublesome where employees are required to or volunteer to work at home beyond the eight-hour day, utilizing employer equipment with GPS technology. Ultimately, a public policy determination will have to be made as whether and to what extent use of GPS technology in employment goes beyond acceptable contemporary societal norms.

One appropriate area for state legislative deliberations with respect to GPS technology is the impact that the technology can have on current state laws which prohibit employment discrimination based on employee

159. *Id.* at ¶ 2.

160. *Id.*

161. *Id.* at ¶¶ 2, 3, 5, 7.

162. Memorandum of Agreement and Stipulation of Settlement, County of Nassau v. Police Benevolent Ass'n of the Nassau County Police Dep't ¶ 2 (Jan. 19, 2007) (on file with author).

163. *See, e.g.*, Otis Elevator Co. v. Local 1, No. 03 Civ. 8862(DAB), 2005 WL 2385849, at *7 (S.D.N.Y. Sept. 23, 2005).

164. *See* Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 624-25 (1989).

off-duty conduct.[165] In general, under these laws, discrimination against an employee for leisure activities is unlawful.[166] However, New York's statute, for example, does not protect an employee's conduct during "paid and unpaid breaks and meal periods" and when the employee is actually engaged in work.[167] In addition, employee activities involving the "use of the employer's equipment or other property" are also excluded from protection.[168] The growing use of GPS technology in employment calls into question the legislative compromise inherent in these types of statutory exclusions. Portable devices, such as cell phones, containing GPS microchips may have the unintended functional result of causing these exclusions to substantially undermine their substantive protections. Finally, the technological capability of employers to track employees engaging in off-duty leisure activities is contrary to the substantive purpose for these laws.

Other industrialized countries have been more aggressive than the United States in examining the privacy implications of employer use of location tracking technologies.[169]

The Article 29 Working Party, an entity established by the 1995 Privacy Directive of the European Parliament and the Council of the European Union has issued an opinion concluding that certain core principles under the Privacy Directive are applicable to an employer's use of GPS technology including: transparency, legitimacy, proportionality, accuracy and retention, security and awareness of staff.[170]

The Article 29 Working Party opinion recognizes that excessive use of external location tracking technologies can erode the distinction between work and leisure time.[171] In applying the principle of

165. MATTHEW W. FINKIN, PRIVACY IN EMPLOYMENT LAW, 422 BNA (2d ed. 2003) (quoting N.Y. LAB. LAW § 201-d2 (McKinney Supp. 1993); *see also* N.Y. LAB. LAW § 201-d (McKinney 2002).

166. *See* N.Y. LAB. LAW § 201-d(2)(c).

167. *Id.* § 201-d(1)(c).

168. *Id.* § 201-d(2)(b).

169. *See generally* Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, *Opinion on the use of location data with a view to providing value-added services*, Working Party 29 Op. No. WP 115 (Nov. 25, 2005) [hereinafter Article 29 Working Party Op. No. 115] (*prepared by* Peter Schaar), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp115_en.pdf (discussing the collection and processing of personal data for the purpose of locating an employee).

170. *See id.* at 9; William A. Herbert, *Privacy and Whistleblower Protections Abroad: The Whole Wide World Is Watching*, 19 U. FLA. J.L. & PUB. POL'Y (forthcoming 2009) (presenting a more detailed analysis of the European approach to workplace privacy issues under the European Convention on Human Rights and EU's Privacy Directive).

171. Article 29 Working Party Op. No. 115 at 10, *supra* note 169.

proportionality from the Privacy Directive, the opinion is critical of employer use of GPS technology when less intrusive means are available.

Another relevant report regarding GPS in employment was issued by the Office of the Privacy Commissioner of Canada in 2006. The report was issued following an investigation into employee complaints over an employer's implementation of GPS technology.[172] The complaints had alleged that the installation and use of GPS technology in the company vehicles of a telecommunications company invaded employees' protected privacy under Canadian law.[173] The Assistant Commissioner concluded that while the technology did result in the collection of employees' personal information, the employer had nonetheless obtained implied consent under Canadian law.[174] The Assistant Commissioner also accepted the employer's proffered rationale for using the GPS technology: productivity, asset protection, and safety.[175] However, the Assistant Commissioner found that an employer's use of the fruits of the technology to evaluate employee performance tipped the balance towards an invasion of privacy.[176] The findings concluded with an expression of concern regarding the cumulative impact new technologies can have on worker dignity and the concomitant importance of employers establishing clear and open policies when implementing GPS technology:

> [O]rganizations, in their quest to be proactive, often resort to technology in anticipation of problems or as a means of maintaining competitiveness. In addition to problems that arise from function creep, the individual's rights are slowly eroded by the cumulative effects of measures intended to meet the bottom line. She cautioned all organizations subject to the Act that the effects on the dignity of employees of all of the measures in place—taken as a whole, not just as one measure along—must be considered in balancing the rights of the individual to privacy and the needs of the organizations to collect, use or disclose personal information for appropriate purposes. She was pleased that the company at the centre of these complaints had taken steps to recognize the dignity of its employees by instituting the policy

172. OFFICE OF THE PRIVACY COMM'R OF CAN., COMMISSIONER'S FINDINGS, PIPEDA CASE SUMMARY No. 351, USE OF PERSONAL INFORMATION COLLECTED BY GLOBAL POSITIONING SYSTEM CONSIDERED (2006), http://www.privcom.gc.ca/cf-dc/2006/351_20061109_e.asp.

173. *Id.*

174. *Id.*

175. *Id.*

176. *Id.* at 6.

on the use of GPS with respect to employee management. Such a measure, she noted, helps maintain that balance in the workplace.[177]

C. LAW AND POLICY REGARDING RFID TECHNOLOGY

Much like GPS, RFID is a form of tracking technology that utilizes microchips containing digital identification information to locate property or employees.[178] Unlike GPS, however, RFID does not rely upon satellite signals but rather the proximity of the microchip to a reader.[179] In 2004, the Bush Administration approved the use of implantable human RFID microchips.[180] Since that time, human RFID microchip implants have been marketed for use in medicine, employment and leisure activities.[181]

The announcement by an Ohio surveillance company, Citywatcher.com, three years ago that it had implanted two employees with RFID microchips illustrates the important need for careful examination and debate regarding the use of RFID technology in employment.[182] In May 2006, in recognition of the substantial privacy and human rights issues associated with mandatory RFID microchip implantation, Wisconsin Governor Jim Doyle signed into law the first statute in the nation banning mandatory implants.[183] One year later, North Dakota became the second state to ban mandatory human microchip implants through a two sentence criminal statute prohibiting a

177. *Id.* at 10.

178. *See* William A. Herbert, *No Direction Home: Will the Law Keep Pace with Human Tracking Technology to Protect Individual Privacy and Stop Geoslavery?*, 2 I/S J.L. & POL'Y FOR INFO. SOC'Y 409, 412 n.7 (2006); RFID JOURNAL, Frequently Asked Questions: What is RFID?, http://www.rfidjournal.com/faq/16/49 (last visited Nov. 22, 2008).

179. *See* Herbert, *supra* note 178, at 412 nn.6-7; RFID JOURNAL, Frequently Asked Questions: How Does an RFID system work?, http://www.rfidjournal.com/faq/17/58 (last visited Nov. 10, 2008).

180. *See* Barnaby J. Feder & Tim Zeller, Jr., *Identity Chip Planted Under Skin Approved for Use In Health Care*, N.Y. TIMES, Oct. 14, 2004, http://query.nytimes.com/gst/fullpage.html?res=9D07EED71F3BF937A25753C1A9629C8B63.

181. *See* European Commission, Information Society and Media, Radio Frequency IDentification RFID: The Internet of Things, 1 (Mar. 2007), http://ec.europa.eu/information_society/doc/factsheets/054-rfid-en.pdf.

182. *See* Richard Waters, *U.S. Group Implants Electronic Tags in Workers*, FIN. TIMES, Feb. 12, 2006, *available at* http://www.ft.com/cms/s/ec414700-9bf4-11da-8baa-0000779e2340.html.

183. *See* Beth Bacheldor, *Wisconsin Governor Signs 'Chip Implant' Bill*, RFID J., June 2, 2006, http://www.rfidjournal.com/article/articleview/2385/1/1/. The Wisconsin statute provides: "(1) No person may require an individual to undergo the implanting of a microchip. (2) Any person who violates sub. (1) may be required to forfeit not more than $10,000. Each day of continued violation constitutes a separate offense." WIS. STAT. ANN. § 146.25 (West Supp. 2006).

"person" from requiring "that an individual have inserted into that individual's body a microchip containing a radio frequency identification device."[184] California's Civil Code now also prohibits involuntary RFID microchip implants[185] and a Missouri prohibition against mandatory RFID implants in employment was signed into law in June, 2008.[186] Similar legislative bans against RFID implants have been introduced in New Jersey and Ohio.[187]

Prior to the Wisconsin, North Dakota, California, and Missouri laws, federal and state laws regulated only the use of RFID microchip implants in animals. A federal program, the National Animal Identification System, tracks farm livestock through RFID technology and has been opposed by farmers throughout the country.[188] New York, for its part, has legislatively restricted the circumstances of when dogs can be implanted with a microchip, and places limits on who can perform the procedure.[189]

A report by the American Medical Association's Council on Ethical and Judicial Affairs underscores the ethical issues connected with human RFID microchip implants.[190] The report noted that such implants can present physical risks to patients including causing interference with electromagnetic devices and defibrillators.[191] In addition, the report

184. Marc. L. Songini, *N.D. Bans Forced RFID Chipping*, COMPUTERWORLD, Apr. 12, 2007, *available at* http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyId=15&articleId=9016385&intsrc=hm_topic. The North Dakota statute provides: "Implanting microchips prohibited. A person may not require that an individual have inserted into that individual's body a microchip containing a radio frequency identification device. A violation of this section is a class A misdemeanor." N.D. CENT. CODE § 12.1-15-06 (Supp. 2007).

185. Renee Boucher Ferguson, *California Law Bans Forced Human RFID Tagging*, EWEEK, Oct. 15, 2007, http://www.eweek.com/article2/0,1759,2198130,00.asp. The statute prohibits a person from requiring, coercing, or compelling another individual "to udergo subcutaneous implanting of a identification device." CAL. CIV. CODE § 52.7(a) (West Supp. 2008).

186. *See* Chris Blank, *New Missouri Laws Limit Gun Range Lawsuits, Employee Microchipping*, NEWS TRIBUNE, Jun. 27, 2008, *available at* http://www.newstribune.com/articles/2008/06/28/news?state/187state02newlaws.txt.

187. NAT'L CONFERENCE OF STATE LEGISLATURES, 2006 PRIVACY LEGISLATION RELATED TO RADIO FREQUENCY IDENTIFICATION (RFID) (2006), http://www.ncsl.org/programs/lis/privacy/rfid06.htm.

188. Theo Emery, *Plan for Tracking Animals Meets Farmers' Resistance*, N.Y. TIMES, Dec. 13, 2006, at A23.

189. N.Y. AGRIC. & MKTS. LAW § 121(2) (McKinney 2004); N.Y. EDUC. LAW § 6705 (McKinney 2001 & Supp. 2008).

190. COUNCIL ON ETHICAL & JUD. AFF., AM. MED. ASS'N, RADIO FREQUENCY ID DEVICES IN HUMANS 1 (2007) *available* http://www.epic.org/privacy/rfid/ama-report.pdf.

191. *Id.* at 2.

found that implants raise privacy and security issues.[192] The Council on Ethical and Judicial Affairs report recommends that physicians provide patients with informed consent about the uncertainties of the implants and take necessary steps to protect patient privacy.[193]

The implantation of microchips is not the only means by which employers utilize RFID technology to track employees. In fact, the few Citywatcher.com employees who refused to accept RFID implants were required to carry a keychain with an RFID microchip.[194] Employers are also inserting microchips into employee nametags and uniforms.[195] The U.S. Postal Service has announced a plan to implement an RFID-tracking system for its industrial vehicles that will include both employee authentication and real time vehicular tracking.[196]

Although some states have considered legislation aimed at regulating the use of RFID technology, these proposals have not targeted the placement of specific limitations on employer use of the technology. New Hampshire has a law prohibiting the use of RFID devices to identify ownership or occupancy of a vehicle.[197] In California, a bill entitled the Identity Information Protection Act of 2006 aimed at regulating the use of RFID technology by state and local governments was vetoed by Governor Arnold Schwarzenegger.[198]

Despite the growing use of RFID technology there have not been any known court decisions regarding the use of RFID technology in employment. In 1999, however, Arbitrator Randall M. Kelly issued a decision and award denying a grievance pursued by a nurses' union challenging the unilateral implementation of an RFID system in Wyckoff Heights Medical Center in Brooklyn, New York.[199] The grievance was denied under the management rights clause of the collective bargaining agreement that permitted the hospital "to make technological improvements."[200]

The nurses' grievance alleged that the hospital's unilateral

192. *Id.*

193. *Id.* at 3.

194. Daniel Sieberg, *Is RFID Tracking You?*, CNN.COM, Oct. 23, 2006, http://www.cnn.com/2006/TECH/07/10/rfid/index.html.

195. BIBBY, *supra* note 2, at 7-8.

196. *See* Beth Bacheldor, *USPS Uses RFID to Manage Vehicles, Drivers*, RFID J., July 10, 2006, *available at* http://www.rfidjournal.com/article/articleview/2478/1/1/.

197. N.H. REV. STAT. ANN. § 236:130(I)-(II) (Supp. 2007).

198. Press Release, Office of the Governor, Legislative Update (Sept. 30, 2006) *available at* http://gov.ca.gov/index.php?/text/press-release/4237/.

199. Wyckoff Heights Med. Ctr. v. N.Y. State Nurses Ass'n, AAA No. 13 300 00122 99 (Aug. 2, 1999) (Kelly, Arb.).

200. *Id.* at 3, 6-7.

imposition of a RFID system to replace an earlier system to locate assigned staff constituted a form of surveillance and a change in an existing term of employment.[201] Under the former system, the unit clerk would contact an assigned staff directly or via an intercom to respond to a patient seeking assistance.[202] Under the RFID-based system, the staff wore badges equipped with RFID microchips that enabled the hospital to pinpoint the location of all staff on a master station screen, thereby speeding the response time to a patient's call button.[203] In addition, the RFID-system provided hospital management with computer-generated reports outlining the specific location and responses by all staff required to wear the badges.[204] These reports have assisted the hospital when responding to patient complaints relating to the quality of care.[205] In denying the grievance, Arbitrator Kelly concluded that although the RFID system had the potential to be used for indiscriminate surveillance, the hospital was utilizing it only as a more efficient means to communicate with staff and to insure quality patient care.[206] Therefore, the system constituted a technological improvement permissible under the management rights clause of the contract.[207]

Labor unions in both Great Britain and Germany have challenged the use of RFID technology by questioning, *inter alia*, the accuracy of the technology and citing to the adverse impacts such technology can have on employees.[208] Due to activism in the area by Great Britain's general union, the GMB, the European Commission created a RFID Stakeholders Group to study the use of tags with RFID chips in employment and to publish recommendations relating to privacy and security issues associated with the technology.[209]

The privacy implications of RFID technology warrant study and possible legislative action to regulate use of the technology in employment. Indeed, substantial privacy concerns have already been documented.[210] Specifically, in a May 2006 report entitled "The Use of

201. *Id.* at 2-3.
202. *Id.* at 4.
203. *Id.* at 4-5.
204. *Id.* at 5.
205. *Id.* at 6.
206. *Id.* at 6-7.
207. *Id.*
208. BIBBY, *supra* note 2, at 9.
209. *Is 'Tagging' Employees a Breach of Privacy?*, WORKPLACE L. NETWORK, Mar. 22, 2007, http://www.workplacelaw.net/display.php?resource_id=8396.
210. *See* Mary Catherine O'Connor, *DHS Subcommittee Advises Against RFID*, RFID J., May 22, 2006, http://ww.rfidjournal.com/article/articleview/23601/1 (arguing that there are real privacy concerns when using RFID-enabled documents).

RFID for Human Identity Verification," the U.S. Department of Homeland Security's own privacy subcommittee questioned the benefits of RFID technology in tracking individuals.[211] Notably, although the subcommittee found certain advantages in utilizing RFID technology, it nevertheless concluded that the overall adverse impact on privacy outweighed those benefits.[212]

In 2004, Ontario Information and Privacy Commissioner Ann Cavoukian issued a report focusing specifically on the privacy implications of RFID technology.[213] Two years later, in June 2006, Commissioner Cavoukian published ten basic privacy guidelines applicable to the use of RFID technology: accountability; identification purposes; consent; limiting collection; limiting use, disclosure, and retention; accuracy; safeguards; openness; individual access; and challenging compliance.[214]

Like GPS, RFID technology enables employers to closely monitor employee movement during both work and breaks and can be used to track protected activities as well as bathroom use. RFID technology, used in conjunction with other surveillance tools, may have a substantially adverse impact on recognized Fourth Amendment protections for public employees in their workplace.[215] Based on the reasonable expectation of privacy standard applied in *O'Connor v. Ortega*,[216] a public employer's broad implementation of RFID technology may result in judicial determinations that the data collected from the technology has violated a constitutionally-protected right to privacy in the workplace.[217]

Lastly, studies demonstrating that RFID technology is susceptible to computer viruses and hacking underscores the importance of careful evaluation and study prior to the ubiquitous implementation of the

211. *Id.*; DATA PRIVACY & INTEGRITY ADVISORY COMM., DEP'T HOMELAND SEC., THE USE OF RFID FOR HUMAN IDENTITY VERIFICATION 2 (Dec. 6, 2006), http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_rpt_rfid_draft.pdf (last visited Oct. 16, 2007).

212. O'Connor, *supra* note 210.

213. *See generally* ANN CAVOKIAN, TAG YOU'RE IT: PRIVACY IMPLICATIONS OF RADIO FREQUENCY IDENTIFICATION TECHNOLOGY (2004), http://www.ipc.on.ca/images/Resources/up-rfid.pdf.

214. ANN CAVOUKIAN, PRIVACY GUIDELINES FOR RFID INFORMATION SYSTEMS (RFID GUIDELINES) 3-4 (2006), *available at* http://www.ipc.on.ca/images/Resources/up-rfidgdlines.pdf.

215. O'Connor v. Ortega, 480 U.S. 709, 717 (1987) ("Individuals do not lose Fourth Amendment protections merely because they work for the government instead of a private employer.").

216. 480 U.S. 709 (1987).

217. *See id.* at 718.

technology in employment.[218]

D. LAW AND POLICY REGARDING BIOMETRICS

The final emerging technology to be examined in this article, biometrics, refers to identification technology that stores and analyzes individual biological characteristics known as "biometric identifiers." Biometric identifiers include hand and fingerprint images, and voice or iris recognition data.[219] The implementation of biometric technology at the Statute of Liberty for security purposes is a symbolic indicator of how far this technology has penetrated our society.[220]

Professor Amitai Etzioni has advocated the use of a national identification card containing a biometric identifier in the United States.[221] He views an identification card as a reasonable balance between community needs and individual liberties, and also as a means of curtailing such things as illegal immigration, credit card fraud, and identity theft.[222] In Professor Etzioni's view, biometric technology would provide an effective means for securing an individual's identity.[223] U.S. Senator Charles Schumer has proposed a nationwide biometric employment card system that would include retinal or fingerprinting scanning as a policy measure designed to combat illegal immigration.[224]

In 2007, Congressmen Luis Gutierrez and Jeffrey Flake introduced a bill entitled the Security Through Regularized Immigration and a Vibrant Economy ("STRIVE") Act, which included a proposed mandate for Social Security cards to contain biometric identifiers as a means to assist in immigration law enforcement with respect to employment.[225]

218. *See* Melanie R. Rieback et al., *Is Your Cat Infected with a Computer Virus?* § 4, http://www.rfidvirus.org/papers/percom.06.pdf (last visited Oct. 16, 2007) (stating that the trust that RFID receives is unfounded based on its susceptibility to hacking).

219. Peter A. Buxbaum, *The Biometrics Dilemma*, HOMELAND SECURITY, Jan./Feb. 2005, at 15.

220. *See* Brian Bergstein, *Biometrics Begin to Enter Daily Life*, ALBANY TIMES UNION, Aug. 12, 2004, at B3.

221. AMITAI ETZIONI, THE LIMITS OF PRIVACY 103-04 (1999).

222. *See id.* at 107-08, 110-11.

223. *Id.* at 125 ("[R]eliable universal identifiers-especially biometric ones-could go a long way toward ensuring that people are secure in their identity . . . .").

224. Maury Thompson, *Schumer Proposes Employment ID Card*, POST-STAR.COM, Apr. 10, 2007, http://www.poststar.com/articles/2007/04/10/news/latest/doc461bbfb88fb74335145294.prt.

225. *See* Security Through Regularized Immigration and a Vibrant Economy Act, H.R. 1645, 110th Cong. § 301(a) (2007); Doris Meissner & James Ziglar, *The Winning Card*, N.Y. TIMES, Apr. 16, 2007, at A19, *available at* http://www.nytimes.com/2007/04/16/opinion/16meissner.html?pagewanted=print.

Under the proposal, the Commissioner of Social Security and the Secretary of Homeland Security would be required to conduct a "privacy impact assessment" regarding the proposed biometric card system.[226] Two former Immigration and Naturalization Service Commissioners, one who is currently the chief executive of a biometric technology company, have publicly supported the proposed biometric Social Security card, describing it as "The Winning Card."[227]

At least three states, Texas, Washington, and Illinois, have been legislatively proactive regarding privacy concerns relating to biometrics. In Texas, it is unlawful to utilize biometric information for commercial purposes without an individual's consent.[228] In Washington, statutory limitations restrict access to biometric information collected by motor vehicle officials.[229] Under Illinois' Biometric Information Privacy Act, private entities in possession of biometric information must develop a written policy which establishes both a retention schedule and guidelines for the permanent destruction of the biometric identifiers and information.[230] In addition, the law mandates informed written consent in advance of a private entity obtaining a person's biometric identifier or information.[231] Furthermore, the law prohibits the sale and restricts the disclosure of a biometric identifier and information.[232]

In the employment context, biometric technology is marketed as a computer-based replacement for the traditional time clock, and as a security enhancement.[233] It remains unsettled whether the imposition of biometric technology in employment constitutes a mandatory subject of bargaining under the NLRA. If biometric technology is determined by the NLRB to constitute a mere replacement for prior non-digital forms of time keeping (such as time clocks or sign-in sheets), the decision to implement biometric systems may be held to be a non-mandatory subject of bargaining.[234] A different legal conclusion may result if bodily

226. H.R. 1645 § 274A(b)(8).

227. *See* Meissner & Ziglar, *supra* note 225.

228. TEX. BUS. & COM. CODE ANN. § 35.50(b) (Vernon 2002).

229. WASH. REV. CODE ANN. § 46.20.037(1), (5)-(6) (West 2001).

230. ILL. COMP. STATE § 740(5)(a) (West 2008).

231. *Id.* § 740(5)(b).

232. *Id.* § 740(5)(c).

233. Stephanie Armour, *Biometrics to Imprint Job Site*, USA TODAY, Dec. 5, 2002, at B3, *available at* http://site.sureid.net/Resources/Bio_job_site.htm; Biometric Time Clocks, http://www.e-biometrictimeclocks.com/ (last visited Oct. 16, 2007).

234. *See* Rust Craft Broad. of N.Y., Inc., 225 N.L.R.B. 327, 327 (1976) (holding that the implementation of time clocks, which replaced the practice of employees manually transcribing their hours onto a timecard, was merely a more efficient and reliable method to enforce workplace rules; thus, there was no requirement for the employer to bargain).

intrusions are associated with the applicable biometric identifier.

In response to New York City's multi-million dollar experiment in the use of biometrics to monitor employee time and attendance, the New York City Council held a hearing in January 2007.[235] At the public hearing, union representatives for city workers expressed strong objections and encouraged the City Council to pass a law prohibiting the City from using biometrics in employment.[236]

In 2007, a federal judge in Iowa denied an application by a railway union seeking an injunction, under the Railway Labor Act[237] ("RLA"), to stop a railroad's implementation of iris recognition technology.[238] The employer's purpose in implementing the biometric system was to improve attendance record keeping.[239] Basing his decision on the RLA's jurisdictional distinction between a "major dispute" regarding efforts to secure a contract and a "minor dispute" relating to contract interpretation, U.S. District Court Judge Bennett concluded that the union's claim was a "minor dispute" because the topic of technological change had been the subject of earlier contractual language.[240]

Biometric technology is also being adopted rapidly throughout the globe for use in e-passports and other forms of identity verification.[241] In the United States, federal and local governments are mandating or utilizing biometric technology with respect to applicants for public assistance and drivers' licenses, and also for immigration purposes.[242] To date, challenges in state courts to state-mandated biometric identification for public assistance have been unsuccessful.[243]

Similar to privacy concerns around RFID technology, the privacy implications of biometrics have been the subject of reports and actions by government officials in Canada, Europe, and Australia.[244] In 1999,

235. Sewell Chan, *New Scanners for Tracking City Workers*, N.Y. TIMES, Jan. 23, 2007, at B1.

236. *Id.*; Michelle Nichols, *N.Y. Scanners Spark Union Cries of "Geoslavery"*, MSNBC.COM, Jan. 26, 2007, http://www.msnbc.msn.com/id/16832030/ (last visited Dec. 15, 2008).

237. 45 U.S.C. §§ 151-88 (1996).

238. Bhd. of Maint. of Way Employees Div. of Int'l Bhd. of Teamsters v. Union Pac. R.R., 475 F. Supp. 2d 819, 821-22, 844 (N.D. Iowa 2007).

239. *Id.* at 824.

240. *Id.* at 838-41.

241. *See* Vivian Yeo, *Biometrics Use to Accelerate in 2006*, CNET NEWS.COM, Feb. 2, 2006, http://news.com.com/Biometrics+use+to+accelerate+in+2006/2100-1029_3-6034384.html.

242. *See* USA PATRIOT Act, 8 U.S.C. § 1379 (2004); Enhanced Border Security and Visa Entry Reform Act of 2002, 8 U.S.C. § 1732(b)(2)(A) (2002); WASH REV. CODE ANN. § 46.20.037 (West 2001).

243. *See, e.g.*, Sheyko v. Saenz, 5 Cal. Rptr. 3d 350, 365 (2003); Medvedev v. Wing, 671 N.Y.S.2d 806, 808 (App. Div. 1998).

244. *See generally* ANN CAVOUKIAN, PRIVACY AND BIOMETRICS (1999), *available at* http://www.ipc.on.ca/images/Resources/pri-biom.pdf; Working Party on the Protection of

Ontario Commissioner Cavoukian issued a report regarding the privacy implications of biometrics.[245] Four years later, the Article 29 Working Party issued a working document analyzing biometrics under the principles of the EU's Privacy Directive.[246] In 2006, in response to concerns regarding biometric privacy, Australian Privacy Commissioner Karen Curtis approved a biometrics privacy code.[247]

European Data Protection Supervisor Peter Hustinx has expressed skepticism regarding the reliability of biometric information.[248] This skepticism is justified, as the research of Clarkson University Associate Professor Stephanie C. Schuckers demonstrates that biometric identification systems can be defeated.[249]

Based on the growing use of biometric technology, along with the genuine questions regarding privacy and reliability, it is vitally important that this technology, like GPS and RFID, be the subject of careful and sober evaluation and analysis.

E. CONCLUSION: THE NEED FOR DISCERNING GOVERNMENTAL ACTION

During the creative marketing and implementation of personal computers in the workplace over the past two decades, there was little discussion regarding the potential adverse impact on employee privacy, or the possible decline in productivity, attributable to widespread e-mail and internet access by employees. In contrast, there remains a genuine opportunity for the development and application of proactive legislation, administratively-imposed or negotiated policies, along with creative technological architecture, to avoid similar problems with respect to the implementation of newer forms of employment technologies. As we have seen *supra*, agreements have been reached between some employers and unions that place limits and protocols on the use of GPS

Individuals with Regard to the Processing of Personal Data, *Working Document on Biometrics*, No. WP 80 (Aug. 1, 2003) [hereinafter Article 29 Working Party No. WP 80] (*prepared by* Stefano Rodotà), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp80_en.pdf; BIOMETRICS INSTITUTE PRIVACY CODE (2006), *available at* http://www.biometricsinstitute.org/displacommin.cfm?an=1&subarticlenbr=8.

245. *See* CAVOUKIAN, *supra* note 244.

246. Article 29 Working Party No. WP 80, *supra* note 244.

247. BIOMETRICS INSTITUTE PRIVACY CODE (2006), *available at* http://www.biometricsinstitute.org/displacommin.cfm?an=1&subarticlenbr=8.

248. *See* Interview by Johnny Ryan with Peter Hustinx, Supervisor, European Data Protection (May 21, 2008), *available at* http://johnnyryan.wordpress.com/2008/05/21/my-interview-with-peter-hustinx-european-data-protection-supervisor/.

249. *Biometric Expert Shows an Easy Way to Spoof Fingerprint Scanning Devices*, PHYSORG.COM, Dec. 11, 2005, http://physorg.com/news8954.html.

technology in the workplace.

As George Washington University Professor Jeffrey Rosen has noted, employees "experience a dignitary injury when they are treated like the inhabitants of the Panopticon."[250] Professor Hoopes has noted that employer overuse of new surveillance technologies may result in the further resurgence of employee activism.[251]

Technological dehumanization, whether intentional or unintentional, has already led to employee anger and protests. Great Britain's general union, the GMB, has expressed strong opposition to the use of RFID and has threatened to strike over the use of the technology.[252] Both cab drivers and municipal professional employees in New York City have held separate demonstrations challenging the implementation of various forms of tracking technologies.[253] In New York City and Philadelphia, cab drivers have gone on strike to protest the implementation of GPS technology.[254] In Massachusetts, twenty state building and engineering inspectors were suspended for insubordination for their refusal to accept cell phones containing GPS technology.[255] The employees took their wildcat action despite an agreement between their employer and union regarding the implementation of the technology.[256]

The fundamental problems associated with emerging technologies that can be utilized to encroach on reasonable employee expectations to privacy and autonomy should be self-evident. As a practical matter, few individuals want to be subject to perpetual surveillance as a condition of employment. Nevertheless, the resiliency of the at-will doctrine, along with contemporary level of union density in the private sector

250. JONATHAN ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 214 (Random House 2000).

251. *See* Hoopes, *supra* note 7.

252. *Union Wants European-Wide Ban on RFID Employee-Tracking*, RFID GAZETTE, July 19, 2005, http://www.rfidgazette.org/2005/07/union_wants_eur.html; Andy McCue, *Union Calls for European Ban on Staff-tracking RFID*, SILICON.COM, July 19, 2005, http://hardware.silicon.com/servers/0,39024647,39150564,00.htm.

253. *See* David Seifman, *Union 'Nay Palm' – Slap at New City Scanners*, N.Y. POST, Aug. 9, 2006, at 12; Matt Friedman, *Cabbies Rally Against GPS Tracking Mandate*, NEWSDAY (N.Y.), Mar. 21, 2006, at A14.

254. *See, e.g.*, John Sullivan, *New York Taxi Strike Causes Longer Waits*, N.Y. TIMES, Sept. 6, 2007, http://www.nytimes.com/2007/09/06/nyregion/05cnd-taxi.html?_r=1&oref=slogin; Athena D. Merritt, *Phila. Cab Drivers Protest Changes with Strike*, PHILA. BUS. J., May 16, 2006, *available at* http://www.bizjournals.com/philadelphia/stories/2006/05/15/daily20.html.

255. Andrea Estes, *20 Inspectors Suspended Over GPS*, BOSTON GLOBE, July 11, 2006, at B1, *available at* http://www.boston.com/news/local/articles/2006/07/11/20_inspectors_suspended_over_gps/.

256. *Id.*

nationwide, renders it likely that employer implementation of emerging technologies will remain unchecked absent governmental action.

As noted earlier, advanced technologies have the real potential of transforming modern workplaces into a twenty-first century rendition of Bentham's Panopticon. Whether the imposition of perpetual technological transparency is consistent with our society's values constitutes a public policy issue meriting careful study and further deliberations. The conduct of sober governmental analysis of these new technologies is also important to examine the correlation between such technologies and the documented increase in workplace stress.

In most of the industrialized world, governments have established privacy offices or commissioners with responsibility for examining new technologies and evaluating their privacy impacts. These governmental privacy offices have issued reports, guidelines, and decisions to regulate the manner in which new technologies can be introduced and applied.

In contrast, in the United States there are few analogous privacy offices with the power and authority to examine the implications of new technologies. Nevertheless, there remains a need for the creation of public entities with the explicit mission to evaluate new technologies and formulate appropriate public policies and guidelines to respond to their potential impact and consequences. As demonstrated *supra*, federal and state policies with respect to genetic testing and discrimination were successfully developed through careful study by temporary legislative and executive bodies.

California has an Office of Privacy Protection within the state Department of Consumer Affairs that provides assistance to consumers and others regarding identify theft and other invasions of privacy.[257] The Office's statutory mission includes providing public education to consumers, providing recommendations regarding privacy policies and practices related to consumers, and promoting mediation procedures for the resolution of privacy related disputes.[258] Absent from the agency's statutory mandate is responsibility for examining workplace privacy issues, as well as analyzing new technologies to determine their potential impact on protected privacy interests.[259]

Legislative bodies and commissions constitute another valuable means of developing public policy with respect to both the privacy and productivity implications of new technologies. Legislative staff with

257. California Office of Privacy Protection, www.privacy.ca.gov (last visited Oct. 16, 2007).

258. CAL. BUS. & PROF. CODE § 350(c), (e)(3) (West 2003).

259. *Id.* § 350(a)-(d).

specialized training and experience can study the new technologies and propose regulatory or voluntary means for using the new technologies in a manner that balances the respective interests of employers and employees.

In the alternative, programs can be established within pre-existing publicly funded research facilities, which support the development of technological innovation, to examine the implications connected with the introduction of new technologies in employment. Such facilities employ professionals with valuable technological knowledge who can be utilized to assist in the development of policies, protocols, software and workforce training aimed at meeting the needs of both employers and employees.

Whether the development of policy and guidelines regarding new technologies in employment is conducted through an executive branch agency, a legislative body or a research facility, it is preferable to the uncertainty of piece-meal litigation that lead to judicially imposed results.

Finally, the absence of regulation does not preclude employers from voluntarily utilizing the principles applicable in workplaces in other countries. Although an employer's embrace of such principles would be unenforceable in most American work settings, the principles can provide an employer with an important means of prudent self-regulation. For example, prior to purchasing or implementing a new technological tool for monitoring, an employer can conduct an analysis of the potential adverse impact the technology may have on employee interests and expectations, including the intrusion into their private lives. Such a study would be similar to the one recommended by the United Kingdom's Information Commissioner's Office ("ICO").[260] The assessment would focus the employer on examining the business justification for the new technology and determine whether there are less intrusive means of meeting that need thereby avoiding the impairment of reasonable employee privacy interests, avoiding an increase in employee stress and avoiding potential employer violations of statutory limitations on workplace surveillance. Following such an analysis, an employer would be better equipped to determine whether the potential benefits of implementing the technology outweigh the potential adverse consequences. Transparency during the employer's assessment, through

260. The Employment Practices Code, Part 3—Monitoring at Work, http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/coi_html/english/employment_practices_code/part_3-monitoring_at_work_1.html (last visited Dec. 26, 2008).

labor-management discussions or other forms of active employee involvement, may aid in avoiding potential disputes and demoralization stemming from the ultimate introduction and application of new technology. Finally, notification to and training of the workforce can assist in the development of technological protocols that can help avoid unnecessary intrusions into employee interests and help stem adverse reactions to the new implementation of workplace technology.