AMERICAN BAR ASSOCIATION, LABOR & EMPLOYMENT LAW SECTION
NATIONAL CONFERENCE ON EQUAL EMPLOYMENT OPPORTUNITY LAW
NEW ORLEANS, LOUISIANA, APRIL 7, 2011

INTERNATIONAL PRIVACY ISSUES PANEL:
TECHNOLOGY IS NOT ALWAYS YOUR BEST FRIEND

THE INFORMATIZATION OF THE BODY: WHAT BIOMETRIC TECHNOLOGY COULD REVEAL TO EMPLOYERS ABOUT CURRENT AND POTENTIAL MEDICAL CONDITIONS

Rachel J. Minter, Law Office of Rachel J. Minter, New York, New York*

Recent years have seen the advent of increasingly sophisticated technology for monitoring and surveillance of employees at the workplace and during work hours – and, increasingly, outside of both.

Employers are scrutinizing the computer use of its workforce through keystroke monitoring;[1] by auditing computers to check which websites are accessed or what has been downloaded or viewed;[2] and by viewing employees' blogs or personal websites and their activity on social networking sites such as MySpace, Facebook and Linked In.[3] One of the most-contested issues in privacy law in the United States is whether an employer can monitor any e-mail sent or received

---

* Rachel Minter has practiced labor and employment law for over 30 years. Ms. Minter represented a union of municipal architects and engineers challenging New York City's refusal to bargain over implementation of biometric hand-geometry scanners. She has spoken on advanced technological monitoring in the workplace at the ABA Section of Labor and Employment Law and its committees and the National Academy of Arbitrators, among other organizations.

[1] Brahmana v. Lembo, 2009 U.S. Dist. LEXIS 42800 (N.D. Cal.) (employer used monitoring tools such as LAN analyzers and key loggers to obtain the password to the plaintiff's personal email account.

[2] *See, e.g.*, Thygeson v. U.S. Bancorp, 2004 U.S. Dist. LEXIS 18863 (D. Ore.).

[3] Pietrylo v. Hillstone Restaurant Group, 2008 U.S. Dist. LEXIS 108834 (D.N.J. 2008); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002).

through its servers, even e-mail sent to or from personal sites such as *gmail* or *AOL*.[4]

In addition to technologies that assist employers with monitoring employees' actions using a desktop or on the Internet, there are two types of technologies that account for the physical presence and movements of an employee. The first, biometric technology, identifies (or verifies the identity of) an employee by scanning a part of the body and recording and storing a digitalized representation of biological traits. "Location-awareness" technologies – Global Positioning Systems, cell phone signals, Radio Frequency Identification Devices – track an employee's movements around and outside the office from signals emitted by something she carries, wears on her person or uses.

Concerns about the ever-increasing use of high-tech tracking devices in American workplaces – what one scholar has termed "Geoslavery" [5] – has continued to rise. Use of these technologies has prompted criticism about the implications for employee morale,[6] the intrusion on personal privacy,[7] incursion on Fourth Amendment protections [8] and erosion of union collective

---

[4] *See*, Stengart v. Loving Care, Inc., 408 N.J. Super. 54, 973 A.2d 390 (N.J. App 2009), *aff'd as modified*, 201 N.J. 300, 990 A.2d 650 (Supreme Court N.J. 2010) (employee's expectation of privacy held subjectively reasonable, because she used a personal e-mail account and did not save the password, and also objectively reasonable, because the computer-use policy was ambiguous and did not warn employees that the contents of personal, web-based e-mails are stored on a hard drive and can be forensically retrieved and read); Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC, 587 F. Supp. 2d 548, 552-53 (S.D.N.Y. 2008) (employer prohibited from using e-mail from employee's personal hotmail and gmail accounts as evidence; company handbook only warned no right of personal privacy in any matter "stored in, created on, received from, or sent through or over the system" but the e-mails at issue were located on, and accessed from, third-party communication service provider systems, were not stored on the company's system, and not necessarily created or sent from the company).

[5] Herbert, William A., *No Direction Home: Will The Law Keep Pace With Human Tracking Technology to Protect Individual Privacy and Stop Geoslavery?*, I/S: A Journal of Law and Policy for the Information Society, Volume 2, Issue 2, page 409 (2006).

[6] Herbert, William A., *Emerging Technology and Employee Privacy: Symposium: the Impact of Emerging Technologies in the Workplace: Who's Watching the Man*, 25 Hofstra Lab. & Emp. L.J. 355 (Spring, 2008). Chan, Sewell, *New Scanners for Tracking City Workers*, The New York Times, Jan. 23, 2007, page B1; Nichols, Michelle, *N.Y. Scanners Spark Union Cries of 'Geoslavery*,' MSNBC.com, Jan. 26, 2007 (http://www.msnbc.msn.com/id/16832030/).

[7] Yung, Jill, *Big Brother IS Watching: How Employee Monitoring in 2004 Brought Orwell's 1984 to Life and What the Law Should Do About It*, 36 Seton Hall Law Review163 (2005); Kaupins and Minch, *Legal and Ethical Implications of Employee Location Monitoring*, Proceedings of the 38th Hawaii International Conference on System Sciences (2005).

[8] People v. Weaver, 909 N.E.2d 1195, 882 N.Y.S.2d 357 (2009).

bargaining rights.[9]

However, to date there has been insufficient scrutiny of the way in which biometric (and, to a lesser-extent, location-awareness) technologies could reveal information about medical treatment, medical conditions, potential medical conditions and non-identified disabilities. Outside of the scientific literature and the U.S. military-security complex, most studies of medical implications of biometrics have been conducted outside the United States – not surprising, as other parts of the world have been far ahead of the U.S. on technological privacy issues in general. The European Union, as well as non-E.U. countries, have considered not only the issue of personal information revealed from biometric identifiers, but have adopted strict standards for the transmission and protection of data gathered by biometric or other monitoring technologies.[10]

As the situation currently stands in this country, employees forced to submit to these forms of monitoring remain vulnerable to consequences such as discrimination on the basis of these characteristics or classifications, or exclusion by carriers or employers from insurance coverage because of potential expenses for treatment. The situation will only become more acute as incursion of biometric and location-awareness systems into the workplace proceeds at a rapid pace and as the technology becomes ever more sophisticated.

I. THE TECHNOLOGY OF BIOMETRICS

---

[9] *See, e.g.*, California State Employees Association v. State of California (Youth Authority), 23 PERC ¶30,114, 1999 PERC (LRP) LEXIS 127 (1999); Teamsters Local 174 v. King County, Case No. 18957-U-04-4823, Dec. No. 9204 (January 12, 2006) (http://www.perc.wa.gov/databases/ulp/9204.html); Civil Service Technical Guild, Local 375 v. City of New York, 58 A.D.3d 581; 872 N.Y.S.2d 442 (First Dept. 2009), *vacating* 40 NYPER (LRP) P7527, 2007 NYPER (LRP) LEXIS 124 (Supr Ct. New York Cnty, 2007).

[10] *See, e.g.*, Regulation (EC) No 45/2001 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, 18 December 2000, published in Official Journal of the European Communities, 12.1.2001.

The term "biometrics" refers to computer-based technology that measures unique biological traits or physical characteristics for the purpose of identification.[11] The unique biological traits or physical characteristics that are measured are known as "biometric identifiers." These include:

- Hand Geometry – Measuring and recording the length, width, thickness, and surface area of the hand.[12]

- Facial Recognition – Characteristics such as the distance between the eyes, the length of a nose, and the angle of the jaw.[13] Of all the biometric technologies, face recognition is the least technologically developed and regarded as the most alarming because of its capability for remote capture of the biometric identifier; at some point the technology will be sophisticated enough to analyze images caught by hidden security cameras.[14]

- Fingerprints – digitalized images, as opposed to "rolled ink" fingerprints, are captured and scanned.

- Voice Recognition (also known as "Speaker Authentication," is a different modality than "speech recognition," which recognizes words as they are articulated and is not a biometric identifier) – Vocal recognition technology identifies people based on the differences in the voice resulting from physiological differences (the physical structure of an individual's vocal tract) and behavioral characteristics of the individual (learned speaking habits).[15]

- Retina Scans – Biometric retina recognition is based on the comparison of the complex pattern of blood vessels located at the back of the eye. Infrared light illuminates the vascular network of the retina and this image is reflected back to the sensor as a wavelength; the algorithm then creates a unique template based on the

---

[11] Additional information and resources on biometrics can be found at the website of the National Science and Technology Council at http://www.biometrics.gov/.

[12] Publication of National Science and Technology Council, Committees on Technology and Homeland Security, Subcommittee on Biometrics. http://www.biometrics.gov/Documents/HandGeometry.pdf.

[13] Porter, Amanda, *Technology & Privacy: Five Great Threats*, University of Texas at Austin, Science, Technology and Society, unpublished paper for the RGK Foundation.

[14] *Biometrics at the Frontiers: Assessing the Impact on Society*, report for the European Commission Joint Research Centre, Institute for Prospective Technological Studies (2005), http://ipts.jrc.ec.europa.eu/publications/pub.cfm?id=1235.

[15] *Biometrics: Enhancing Security or Invading Privacy?* The Irish Council for Bioethics (2009), pp. 72-73, at http://www.bioethics.ie/uploads/docs/Final_Biometrics_Doc_HighRes.pdf.

blood vessel pattern of the retina.[16]

• Iris Scans – an infrared camera illuminates the visible, colored part of the eye and creates an image that is converted into digital templates.

• Vein Scans – the pattern and structure of blood vessels visible on the back of an individual's hand or finger are captured, the algorithm registers the vascular pattern characteristics (blood vessel branching points, vessel thickness and branching angles) and stores these as a template for comparison with subsequent samples from the enrolled individual.

In order to enroll in the system, the employee must submit to having a template made of the biometric identifier. Despite frequent assurances by employers, creating a biometric template is not a completely benign process. Creating a template of the iris, for example, requires infra-red illumination and capturing its image with a camera held 8-13 inches from the employee's eye.[17] It has been reported that retinal scanning could cause thermal injury on the back of the eye.[18]

The template created is stored in a system and is then read by data collection devices ("DCD's) such as sensors or scanners. The next time the person "interfaces" with the DCD, his or her body part is inserted and verified against the stored template.

II. USING TRACKING TECHNOLOGY IN THE WORKPLACE

Although some DCDs come equipped with security features, such as door-access control or "smart card" readers, biometric technology is more commonly used in workplaces for timekeeping than for security. Biometric equipment marketed to employers to stop "time theft" and "buddy punching" is a multi-million dollar business.[19]

---

[16] *Id*.

[17] Brotherhood of Maintenance of Way Employees Division, IBT v. Union Pacific Railroad, 475 F. Supp. 2d 819 (N.D. Iowa, West. Div. 2007).

[18] *Biometrics at the Frontiers: Assessing the Impact on Society*, report for the European Commission Joint Research Centre, Institute for Prospective Technological Studies (2005), http://ipts.jrc.ec.europa.eu/publications/pub.cfm?id=1235.

[19] http://www.veritasksoftware.com/; http://www.msnbc.msn.com/id/23814798; http://findarticles.com/p/articles/mi_m3495/is_12_53/ai_n31152982/

For example, the Union Pacific Railroad replaced a timekeeper roll-call for its field crews with biometric iris recognition technology. The device is not used for security of the rail yards – only for attendance.[20] Other employers use retina scans for the same purpose. Calandriello v. Tennessee Processing Center, LLC, 2009 U.S. Dist. LEXIS 116613 (M.D. Tenn.).

New York City installed biometric hand-geometry scanners that were little more than high-tech "time clocks" as part of an electronic timekeeping and payroll system for city agencies that as of this writing has cost approximately $700 million.[21] Instead of signing a time sheet, agency employees were required to insert a hand into biometric equipment.[22] Columbia Presbyterian (now NY-Presbyterian) Hospital installed a hand-geometry scanner in 1997 to control physical access and to monitor employee attendance.[23]

Other biometric devices being marketed to employers to monitor employee "efficiency" include a fingerprint-reading computer mouse[24] and a computer that reads hand veins from a sensor in the keyboard.[25]

Increasing numbers of employers are utilizing location-awareness technology, in addition to or in lieu of biometrics, to monitor employees. Global Positioning Systems (GPS) are most frequently found in the workplace as navigation devices in employer-owned vehicles, or inside employer-issued cell phones or hand-held communication devices in which the GPS tracking feature

---

[20] Brotherhood of Maintenance of Way Employees Division, IBT v. Union Pacific Railroad, 475 F. Supp. 2d 819 (N.D. Iowa, West. Div. 2007).

[21] http://www.nydailynews.com/ny_local/2009/12/18/2009-12-18_behind_a_bloated_contract_council_will_probe_timeclock_company.html

[22] http://www.nytimes.com/2007/01/23/nyregion/23scanning.html?_r=3

[23] Woodward, John, *et. al.*, *Army Biometric Applications: Identifying and Addressing Social Concerns*, Rand Organization monograph (2001), available at http://www.rand.org/pubs/monograph_reports/MR1237.html.

[24] http://www.engadget.com/2007/06/27/iogear-fingerprint-reading-mouse-with-nano-shield/.

[25] http://www.engadget.com/2007/09/11/fujitsu-palmsecure-mouse-reads-veins-wont-secure-palms/.

has been activated.[26] Radio Frequency Identification Devices (RFIDs) have become significantly prevalent in health care institutions. RFID devices contain tiny microchips, in some cases as small as a grain of sand, which hold unique identifying data, and have a small antenna attached that is read remotely by an RFID reader.[27]

Although a detailed discussion of other technologies is outside the scope of these materials, we note that tracking location also poses problematic privacy concerns. Like biometrics, location-awareness technology can reveal personal information to an employer that it would not otherwise have obtained.

Some information is relatively innocuous: A company with RFID readers installed at doorway access points at regular intervals could learn, for example, whether an employee ate at the company cafeteria or at a restaurant outside the building.[28]

However, if an employee is carrying a company cell phone or hand-held device, wearing an RFID-tagged ID badge, or is inside a GPS-equipped company car that the employee is permitted to drive for personal use, there is a record of where this employee goes and when (even during lunchtime or right after work). Under some circumstances an employer who is tracking employee movements can learn confidential medical information simply by looking at the particular destination.

For example, the employer could suspect that an employee has an alcohol problem because of repeated lunch-hour stops at a local church which hosts an AA meeting at noon, or that an

---

[26] However, cell phone signals can be traced even without the tracking application. *See Department of Education v. Halpin*, New York City Office of Administrative Trials and Hearings, Index No. 818/07, accessed at http://search.citylaw.org/isysquery/8cd123fd-1835-4529-a46e-1e295d603a06/2/doc/ (employer tracked signals from cell phone towers to plot the route and times of the employee's return to his suburban home, which established that he was routinely leaving work hours before the end of his shift).

[27] In one New York City hospital, employees wear RFID-equipped ID badges which emit signals read by scanners in patient rooms and the nurses lounge, enabling it to track the movements of nursing staff around the floor. *Matter of Wyckoff Heights Medical Center and New York State Nurses Association*, AAA Case No. 13 300 00122 99

[28] http://www.rfidgazette.org/2006/10/can_rfid_track_.html.

employee has a serious disease from after-work visits to an AIDS clinic.[29] Similarly, most people are unaware that the "GPS" systems installed in New York City taxicabs have no navigational capability, but simply track the movements of the cab (and, by extension, those of the driver); a noon-time stop on a particular block could reveal that the driver stopped at a mosque to pray rather than at a diner to eat – or that he was visiting a doctor at a hospital specializing in treatment of cancer, Memorial Sloan-Kettering.

III. THE INFORMATIZATION OF THE BODY

Scanning biometric identifiers such as irises, retinas or hand veins can reveal information about existing medical conditions, as well as medical predispositions, based on particular biometric patterns. The vein of data to be mined from biometrics (pun intended) is so rich that one study termed the current climate as "the informatization of the body." [30]

Direct medical implications from the use of biometric technology are considered to be those resulting from potential risks to human health from the use of the technology.[31] Indirect medical implication involves detection of sensitive medical information about a person's health status or characteristics from the biometric identifier.[32] Information of that nature might fall into the hands of employers or insurers as a result of what is called "function creep." "Function creep" has

---

[29] These theses were contained in Renenger, Aaron, *Satellite Tracking and the Right to Privacy*, 53 Hastings L.J. 549, 557 (2002). Though posed by Renenger as a hypothetical, in one case an employee was actually terminated because the employer feared infection by the HIV virus as a result of the employee's volunteer work at an AIDS foundation. Brunner v. Al Attar, 786 S.W.2d 784, 1990 Tex. App. LEXIS 317.

[30] Van der Ploeg, Irma, *Genetics, Biometrics and the Informatization of the Body*, Ann Ist Super Sanità, Vol. 43, No. 1: 44-50 (2007).

[31] *Biometrics at the Frontiers: Assessing the Impact on Society*, report for the European Commission Joint Research Centre, Institute for Prospective Technological Studies (3/2005), available at http://ftp.jrc.es/EURdoc/eur21585en.pdf.

[32] Suomi, R., *Biometrical Identification as a Challenge for Legislation: The Finnish Case*, in Godara, V. (editor), Risk Assessment and Management in Pervasive Computing: Operational, Legal, Ethical and Financial Perspectives, IRM Press (2008); Albrecht, A., *BioVision: Roadmap for Biometrics In Europe to 2010*, National Research Institute for Mathematics and Computer Science (2003), available at http://ftp.cwi.nl/CWIreports/PNA/PNA-E0303.pdf.

variously been defined as "the process by which the original purpose for obtaining the information is widened to include purposes other than the one originally stated"[33] or "the expansion of a process or system, where data collected for one specific purpose is subsequently used for another unintended or unauthorized purpose."[34]

Employers who gather biometric data for timekeeping, access or security might as a result of function creep expand the use of that data for an intended, but unauthorized purpose – to discover information about employees' medical conditions, possible or potential medical conditions, and/or need for expensive medical treatment. While there have been no reported instances of such abuse occurring, the danger is not entirely speculative; it is now known that certain medical disorders, or predispositions to medical conditions, are associated with specific biometric patterns.[35]

What biometric identifiers are known (or suspected) to yield evidence of what medical conditions or predispositions?

- Hand geometry measurement is a potential source of identifying disorders indicated by particular geometry patterns, such as gout and arthritis.[36] Hand geometry can also be an indicator for Marfan Syndrome, an inherited disorder of connective tissue that can affect the heart, blood vessels, eyes, and skeletal system. People with Marfan syndrome are usually tall and thin, with disproportionately long arms, legs, fingers and toes (some experts believe Abraham Lincoln may have had Marfan syndrome).

- Researchers in the field of dermatoglyphics, the study of the patterns of the ridges of the skin on parts of the hands and feet, have identified characteristic fingerprint patterns known to be associated with certain chromosomal disorders, Down

---

[33] Woodward, John, *et. al.*, *Army Biometric Applications: Identifying and Addressing Social Concerns*, Rand Organization monograph (2001), available at http://www.rand.org/pubs/monograph_reports/MR1237.html.

[34] Mordini, Emilio and Massari, Sonia, *Body, Biometrics and Identity*, Bioethics, Volume 22, Issue 9 (November 2008).

[35] *Id.*

[36] *Biometrics in Identity Management*, FIDIS Network of Excellence, http://www.fidis.net/resources/deliverables/hightechid/int-d37001/doc/21/.

Syndrome, Turner Syndrome and Klinefelter Syndrome.[37] Researchers at Johns Hopkins are reported to have found a link between an uncommon fingerprint pattern, known as a digital arch, and a medical disorder called chronic intestinal pseudo-obstruction (CIP).[38]

• The eyes can reveal a variety of health conditions, including AIDS, Lyme disease, congestive heart failure and cholesterol level; even diseases like leukemia, lymphoma, Stevens-Johnson syndrome, and sickle cell anemia can affect the eyes.[39] Pupillary responses can vary if the subject has been drinking or taking drugs or is pregnant.[40]

• Retinal scans measure the blood vessel patterns in the back of the eye, which are subject to the affects of aging and may change with certain medical conditions;[41] retinal micro-vascular signs have been shown to be associated with long-term risks of type 2 diabetes and hypertension, as well as vascular conditions such as stroke and cardiovascular mortality.[42]

• While enrollment and subsequent recognition for biometric iris

---

[37] Hunter, H., *Finger and Palm Prints in Chromatin-Positive Males*, J. Med. Genet. Vol. 5, No. 112 (1968); Woodward, J., *Biometric Scanning, Law & Policy: Identifying the Concerns – Drafting The Biometric Blueprint*, 59 U. Pitt. L. Rev. 97 (Fall, 1997).

[38] Schuster, M., *Gastroenterology: Fingerprinting GI Disease*, Johns Hopkins Physician Update (April 1996), cited in Woodward, *Biometric Scanning, Law & Policy*, *supra*.

[39] House of Commons, Select Committee on Science and Technology, Written Evidence, http://www.publications.parliament.uk/pa/cm200506/cmselect/cmsctech/1032/1032we03.htm.

[40] Ostaff, C., Retinal Scans Do More Than Let You In The Door, PHYSorg.com (August 31, 2005), http://www.physorg.com/news6134.html; National Workrights Institute Newsletter, Volume V, No. Five (Winter 2007-2008); House of Commons, Select Committee on Science and Technology, Written Evidence, *supra.*

[41] House of Commons, Select Committee on Science and Technology, Written Evidence, http://www.publications.parliament.uk/pa/cm200506/cmselect/cmsctech/1032/1032we03.htm.

[42] Nguyen, T., *Retinal Vascular Manifestations of Metabolic Disorders*, Trends Endocrinol Metab. , Vol. 17, No. 7 (2006).

scan systems was generally not affected by acute eye disease, patients with uveitis could pose a problem to iris recognition, particularly if they required pharmacological dilation.[43] Cataract surgery can change iris texture in such a way that iris pattern recognition is no longer feasible or the probability of false rejected subjects is increased.[44]

• It is widely acknowledged that voice recognition technology can reveal anger, nervousness or distress.[45] The Information Commissioner of the Republic of Slovenia has acknowledged the possibility that a company using voice recognition for access control could subsequently use the biometric data collected to ascertain the emotional state of individual employees.[46]

• Scientists already contemplate that facial characteristics may be used to detect a subject's emotional condition from his or her expressions.[47] Face recognition biometrics, like hand geometry, can reveal Marfan syndrome, because patients with Marfan's have a special symmetry parameter of the face geometry.[48]

Medical information can also be derived from the process itself, *i.e.*, problems with enrollment or failure of recognition. First, injuries or illnesses might prevent a person from being

---

[43] Mehmood, Tariq, *et. al.*, *Iris Recognition in the Presence of Ocular Disease*, J. R. Soc. Interface (2009) 6, 489–493 (published online March 11, 2009).

[44] Roizenblatt, Roberto, *et. al.*, *Iris recognition as a biometric method after cataract surgery* BioMedical Engineering OnLine 2004, 3:2, http://www.biomedical-engineering-online.com/content/3/1/2.

[45] *Biometric Identification Technology Ethics*, CSSS Policy Brief, November 2003), accessible at http://danishbiometrics.files.wordpress.com/2009/08/news_2.pdf.

[46] *Guidelines Regarding the Introduction of Biometric Measures*, *supra*.

[47] Mordini E and Ottolini C (2007). *Body Identification, Biometrics and Medicine: Ethical and Social Considerations*, Annali dell Istituto Superiore di Sanità 43(1): 51–60.

[48] *Biometrics in Identity Management*, *supra*.

enrolled and recorded by the system, *e.g.*, eye diseases could prevent iris scanning, arthritis could interfere with measuring hand geometry, finger burns can prevent fingerprinting.[49] Second, medical information can be deduced by comparing selected biometric characteristics captured during initial enrollment and upon subsequent entries; for example, facial geometry measured at different periods of time can reveal some endocrine disorders.[50] In addition, infrared cameras used to create a biometric template may detect surgical modifications to the body because the temperature distribution across reconstructed and artificial tissues is different from normal and thus can easily, and covertly, detect dental reconstruction, plastic surgery, added or subtracted skin tissue, body implants, scar removal, laser-resurfaced skin and removed tattoos.[51]

IV. CONSEQUENCES TO EMPLOYEE OF MEDICAL DISCLOSURE

The consequences for an employee whose existing medical condition, or predisposition to develop that condition, are revealed through biometric scanning to his or her employer could be profound. Such information may affect access to insurance coverage or subject the employee to unlawful discrimination on the basis of disability or perceived disability. One study of biometrics use came to the same conclusion:

> "In addition, by linking the biometric database with other databases (*e.g.* user's credit card transactions), we know where the person has been and at what time. In addition to the personal privacy, there are also concerns that biometric data can be exploited to reveal a user's medical conditions. Such information is privileged that could be potentially used to discriminate [against] some users for employment or benefits purposes (*e.g.*, health insurance)."[52]

Any discrimination by the employer on the basis of the employee's disability or perceived

---

[49] Mordini, Emilio and Massari, Sonia, *Body, Biometrics and Identity*, Bioethics, Volume 22, Issue 9 (November 2008).

[50] *Id*.

[51] *Id*.

[52] Jain, A. and Kumar, A, *Biometrics of Next Generation: An Overview* in Privacy and Technologies of Identity (2006), pp. 117-134 http://biometrics.cse.msu.edu/Publications/GeneralBiometrics/JainKumarNextGenBiometrics_BookChap10.pdf.

disability would be difficult to uncover, let alone prove, for a number of reasons. First, because the information is covertly obtained, the employee is not aware that the employer now has knowledge of his health issues or physical condition. Second, the employer may know even more about her medical history than the employee herself, if the information derived from the biometric identifier relates to a genetic predisposition to develop a disease, and she has not been tested for that gene.

An employee with a disability who does not need accommodation has the choice whether or not to disclose, but that choice is taken away from the employee whose confidential medical information was obtained as a result of unauthorized and unanticipated function creep. Unlike an employee who self-discloses, the one whose biometric data was captured and misused has no opportunity to rebut any perceptions that are based solely on information derived from the biometric identifier. Where the employer has (a) wrongly perceived that a disability exists, because the data that may have been interpreted incorrectly; (b) wrongly perceived that the employee is currently disabled where the biometric data indicates only the possibility that a particular medical condition might develop; or (c) wrongly perceived the severity of the identified medical condition, and thus incorrectly concluded that it affects the employee's ability to perform the essential duties of his position.

Similar concerns arise with acess to health insurance. As the National Workrights Institute once cautioned, "[w]ith the costs of employer-provided medical insurance continuing to rise, employers have a strong financial incentive to access and use" medical information derived from biometric data.[53] An employer may believe that its financial interests will be affected by employing a person who has serious medical conditions, or may develop such conditions down the road, and who is likely to need expensive medical treatment which will be paid by the employer directly (if self-insured) or indirectly (if premiums are experience-rated). Notwithstanding the legal requirements of the ADA or the FMLA, the employer will also anticipate lost productivity from absences when the employee is too ill to work or needs time off for medical appointments.

In its 2009 report the Irish Council for Bioethics noted a "particular concern" about the possibility of "deriving additional health, medical and sensitive personal information from certain biometric identifiers" and the "far-reaching implications" that could have for the individuals

[53] National Workrights Institute Newsletter, Volume V, No. Five (Winter 2007-2008).

involved.[54]

V. PROTECTING AND REGULATING USE OF BIOMETRIC DATA

The privacy issues presented by authorized and unauthorized uses of biometric identifiers have been the subject of several studies prepared by research institutes to assist in formulating government policies. In a number of these studies, and in articles written by European scholars, the issue of improper use of medical information derived from biometric systems has been specifically considered.

Also striking in the responses outside of the United States is consideration of the ethical issues inherent in collecting and using biometric identifiers. "Fair information principles" include the principle of proportionality: That the use of biometrics is "justified in the context of the application, and that no other means of authentication may fulfill equally well the requirements without the need for biometrics." [55] There would presumably be less concern about misuse of medical data when proportionality is considered:

> "For instance when biometric data are processed for access control purposes, the use of such data to assess the emotional state of the data subject or for surveillance in the workplace would not be compatible with the original purpose of collection." [56]

A related principle is the "purpose principle." Article 6 of Directive 95/46/EC provides that:

> "personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. In addition, the personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and further processed" [57]

---

[54] *Biometrics: Enhancing Security or Invading Privacy?* The Irish Council for Bioethics (2009), pp. 72-73, at http://www.bioethics.ie/uploads/docs/Final_Biometrics_Doc_HighRes.pdf.

[55] Mordini, Emilio and Massari, Sonia, *Body, Biometrics and Identity*, Bioethics, Volume 22, Issue 9 (November 2008).

[56] Article 29 – Data Protection Working Party (2003) *Working Document on Biometrics* 12168/02/EN, WP 80, p. 7.

[57] *Id.*

As noted, the European Union has adopted regulations regaring the processing of personal data (see footnote 10, *supra*). Outside the EU, measures to control the gratuitous use of biometrics, and protect the data generated, have been promulgated. Australia's Privacy Commissioner, for example, approved a Biometrics Privacy Code that specifically covers employee records containing biometric information.

The Information Commissioner of the Republic of Slovenia has issued "Guidelines Regarding the Introduction of Biometric Measures," a lengthy and detailed protocol that contains significant protections for both pubic- and private-sector employees. Biometrics use in the public-sector is regulated by statute and biometric measures may be utilized only if they are necessary for security or to protect secret data and this purpose "cannot be achieved by milder means."[58] Private-sector employers are subject to even greater restrictions on implementation, and must notify employees in writing prior to use of the biometric system.[59]

In the United States, legislative protection and regulation of biometrics at the state or local levels is limited, and earlier attempts to broaden it were largely unsuccessful.

The Texas Business and Commercial Code prohibits unauthorized commercial use or disclosure of a "biometric identifier;" any person who "possesses" a biometric identifier must "store, transmit, and protect it from disclosure in at least as protective a manner as other confidential information." [60] In Washington State, the motor vehicle law contains privacy protection and notice requirements for biometric information on drivers' license.[61] Illinois requires private entities in possession of biometric identifiers to develop a written policy establishing a retention schedule and guidelines for permanently destroying the information; to safeguard the biometric data; and to obtain written consent before obtaining a person's biometric identifier or information. The statute also prohibits commercial use of biometric information.[62] Colorado includes "biometric data" in the

---

[58] Guidelines Regarding the Introduction of Biometric Measures, Information Commissioner, Republic of Slovenia (February 29, 2008), Article 79.

[59] *Id.*, Article 81.

[60] Texas Business and Commercial Code § 35.50.

[61] Rev. Code Wash. § 46.20.037.

[62] Ill. Comp. State § 740(5).

definition of "personal identifying information" for which private businesses must have a policy for destruction of records.[63]

A bill introduced in the Georgia legislature, the "Biometric Information Protection Act," would have prohibited both private and public employers from using for identification purposes, or requiring as a condition of employment, any information derived from biometric information or "personal location tracking technologies.[64] A New Jersey bill would have restricted commercial use or disclosure of biometric identifiers; mandated secure storage of data; required a government entity possessing a biometric identifier of an individual to establish a "reasonable procedure" that does not "unduly burden" the user to correct inaccurate information.[65]

---

[63] Colorado Revised Statutes § 6-1-713.

[64] http://www.legis.ga.gov/legis/2007_08/fulltext/hb276.htm.

[65] http://www.njleg.state.nj.us/2002/Bills/A2500/2448_R1.HTM.