VOL. 36, NO. 5/ SUMMER 2011

EMPLOYEE RELATIONS LAW JOURNAL

ASPEN PUBLISHERS

ASPEN PUBLISHERS VOL. 36, NO. 5 SUMMER 2011

Employee Relations LAW JOURNAL

Wolters Kluwer
Law & Business

Employee Relations Law Journal

EDITOR-IN-CHIEF
Steven A. Meyerowitz

EDITOR
Elizabeth Venturo

SENIOR MANAGING EDITOR
Joanne Mitchell-George

PUBLISHER
Paul Gibson

EMPLOYEE RELATIONS LAW JOURNAL (ISSN 0098-8898) (USPS 407-630) is published quarterly by Aspen Publishers, 76 Ninth Avenue, Seventh Floor, New York, NY 10011. One year subscription rate: $469; two year: $797; three year: $1,126; single issue: $141. To subscribe, call 1-800-234-1660. For customer service, call 1-800-234-1660. Address editorial comments to **Employee Relations Law Journal**, 10 Crinkle Court, Northport, NY 11768. POSTMASTER: Send address changes to **Employee Relations Law Journal**, Aspen Publishers, 7201 McKinney Circle, Frederick, MD 21704.

www.aspenpublishers.com

Author Guidelines and Publication Policies

Employee Relations Law Journal (*ERLJ*) is a quarterly subscription-based journal published by Aspen Publishers that primarily focuses on the legal issues associated with human resources management. *ERLJ* is directed to in-house counsel, corporate human resources executives, and attorneys concentrating in employment law. Articles should be written to meet the needs of this audience. *ERLJ* strives to analyze complex information and provide clear, concise analysis and guidance to our readers. Our tone is practical and readable.

Publication Policies. *ERLJ* encourages the submission of manuscripts from experts in the field. Manuscript submission implies a commitment to publish in *ERLJ*. Previously published articles and articles under review by other publications are not acceptable except in rare cases. Articles adapted from book-length works in progress will be considered for prior publication, with attention given to the necessary copyright arrangements.

Guidelines for Authors. Articles should be approximately 15–35 double-spaced pages in length. Extensive endnotes and citations are discouraged. Notes deemed essential should be presented in endnotes double-spaced at the end of the article. Authors are encouraged to talk with the Editor-in-Chief prior to preparing and submitting their articles. Text should be submitted electronically, preferably in Microsoft Word format, either as an email attachment or on a disk. Type subheads flush left, with a one-line space above and below.

Articles should be written in neutral, third-person voice. Articles must appear as continuous prose, with full sentences. Outline format must be converted to ordinary paragraphs with transitional sentences. An author's internal headings should not be relied on as the sole means of making points or transitions.

Excessive use of quotation marks should be avoided. Tables, if any, should be presented on a separate page at the end of the article, not inserted in the text. Each table should be entered in its own computer file. Graphic illustrations must be available as high-quality electronic images.

Authors should attach the following on separate pages: (1) A cover sheet giving the article title and each author or co-author's professional or academic affiliation, current mailing address, telephone number, fax number, and email address; (2) an abstract of 50–75 words; and (3) for each author or co-author, a biographical statement of no more than 50 words, written in the third person.

Submission and Acceptance. Submit one copy of the manuscript to the Editor-in-Chief at the address indicated below (submission of articles via email to the address indicated below is preferred).

PLEASE NOTE: Copyright will be retained by the publisher. All contributors must sign a copyright transfer agreement. Contributors may use the work on a limited basis for their own professional use, except where such use may reasonably be judged to be competitive or substantially harmful to the commercial value of *ERLJ*. Contributors also may post the work on their firm's Web page 30 days after original publication, providing appropriate credit is added.

There is no payment for articles; contributors will receive copies of the issue in which their article is published. Articles are subject to editorial revision for length, clarity, and to conform to the journal's style guidelines. Manuscripts not accepted for publication will not be returned.

Contact Information. To submit articles, or for further information, please contact the Editor-in-Chief:

Steven A. Meyerowitz, Esq.,
President Meyerowitz Communications Inc.
10 Crinkle Court
Northport, New York 11768
631.261.9476 (phone)
631.261.3847 (fax)
SMeyerow@optonline.net

ASPEN PUBLISHERS VOL. 36, NO.5 SUMMER 2011

Employee Relations LAW JOURNAL

Wolters Kluwer Law & Business

Editorial Advisory Board

Privacy—Between the Devil and the Deep Blue Cloud, Trends in Biometric Data Collection and Use

I. Jeffrey Pheterson

The author contemplates trends in biometric data collection and use from the perspective of his grandfather.

My grandfather Max was a carpenter. He was a simple man who came to this country from northern Europe, worked hard and raised his family. He protected his privacy, often in small ways. He did not like the newspaper left at the end of the driveway all day. "They" would know we weren't home. The world was a hostile place—sometimes—that would intrude on our lives, and the less "they" knew about us, the better Max liked it. He was not "a Rockefeller," as he might put it, but our privacy was important, and its protection as a civil liberty was one of the reasons he loved this country.

I often find myself using my grandfather as a benchmark. What would Max think of this or that new development? As for biometric data collection, he and I would have to have a long sit-down discussion.

THE SCOOP ON BIOMETRIC DATA

Briefly stated, biometric data are derived from the personal and unique physical characteristics of each individual. Fingerprints were the first type of biometric data that were collected and catalogued systematically. Technological applications analyzing and using biometric data to authenticate identity are becoming more and more prevalent, and inexpensive. The databases of unique biological identifiers are increasing in size and accuracy day by day.

Max would have two basic questions. First, will this trend continue? Second, is widespread use of this type of data good for us, for the protection of our family and our society?

It is beyond discussion that the use of biometric data is an irreversible, and growing, trend. The utilization of biometric readers in human resources applications is now widespread. Hand scanners have replaced the antiquated punch cards used by Max for decades, just as Google has replaced the *Encyclopedia Britannica*. The old disciplinary problem

I. Jeffrey Pheterson is the Managing Member at Ward Damon Posner Pheterson & Bleau, P.L. He may be contacted at *jpheterson@warddamon.com.*

of one employee "punching in" his or her cohorts, and thus falsifying the time records, prior to their actual appearance to start work is now a thing of the past. The unique biometric fingerprint of the back of one's hand closes that door, forever. No hand print, no "clock in." The cost of this new technology has dropped precipitously, and now these devices are seen in the smallest of workplaces. Newer applications for these data are, as one would expect, exponentially more sophisticated.

APPLICATIONS IN THE 21ST CENTURY

The US Department of Defense Common Access ID Card has been issued to all U.S. service personnel and contractors on US military sites. This card contains biometric data and digitized photographs as well as laser-etched photographs and holograms to add security and reduce the risk of falsification. Use of this type of data at borders and airports would solve many security issues.

The combination of various biometric identification processes increases the probability of accuracy many fold. Using a smart card like the Common Access Card, in tandem with multiplex-enabled equipment would permit crosschecking of different biometric "fingerprints" simultaneously. Patents have been applied for regarding processes that combine touch screen technology for fingerprint identification with cameras for face recognition and sound sensors for voice recognition. Adding retinal scans may not be far behind. Once all of these technologies are merged, the potential for identity deception will be reduced dramatically.

A recent insightful science and technology article in *The New York Times* identified a number of new ways that face recognition technology and video monitoring are being used today.[1] Chronic failures or bottlenecks for quality can be corrected immediately, as the technology is never sleeping, and remains ever vigilant.

The uses noted in the *The New York Times* article are diverse and extremely creative. Correctional officers are helped to assess ongoing potential inmate unrest based on video readings monitored continuously by computers, with staff being kept in touch constantly using smartphones. Health care workers and physicians are reminded instantly to wash their hands before and after touching patients by a computer that monitors activity in patient rooms and that transmits an alert to a handheld devise when a failure to wash hands is detected. Hospital patient facial expressions, in bed, can be monitored to identify discomfort, and such data can be sent to the nursing station without a call button, automatically. Face recognition technology now is so sophisticated that it can be used by filmmakers to sample audience reaction to films—individual by individual, and not only scene by scene, but frame by frame.

The commercial application of this biometric data is well established in public venues. Walt Disney World secures an image of each person entering its gates, and ties that image to the bar code information on

the ticket. Buying and reselling multi-day passes, which had plagued the parks, has been eliminated. Indeed, the use of cameras located throughout London was invaluable in securing arrests related to the recent Tube bombings.

Clearly, there are many extremely beneficial uses for this biometric data. However, as biometric data uniquely identify specific individuals, its misuse or subversion remains a concern.

LOOMING CONCERNS

First, what will happen to the gathering storm of these data that are being collected in one form or another if someone is bent on exposing this personal information? As the recent WikiLeaks experience has shown us all too well, it only takes one errant employee with access to data to download that data to those who are willing to publish it to the Web, and expose it to the world. Julian Assange is the devil to some, and to others he is a cross between Robin Hood and Dan Rather. To Max he would be a self-aggrandizing crook, a contemptible deceiver. WikiLeaks will be dealt with, but the underlying problem is endemic. There are other Assanges out there.

The second basis for concern focuses on the authenticity of the data themselves. Should someone be able to hack in, that person could subvert the data and mask the true identity of the person being scanned or monitored. The security personnel would not know the true identity of the person presenting at the checkpoint or location. The security apparatus will have been circumvented. In that circumstance, the use of this technology actually would hinder this security function, as the person would gain access, and the security system would have sent a false positive identification permitting access. The challenges are real, both from the perspective of legal constraints, and from the point of view of public acceptance.

Companies that collect and use these data, but fail to take appropriate measures to assure its security, may face legal challenges for negligently permitting its improper dissemination. Also, leaks generate a strong negative public reaction. When hackers recently cracked into a database of university donors, there was a very vigorous outcry. Much time and effort was spent to demonstrate how seriously this lapse was taken, and how it would not be repeated.

Many people feel like Max. If he entrusted an institution with his personal data, those data should be kept confidential.

Some companies have chosen voluntarily to limit the type or amount of data retained or available for analysis. Recently, Google launched its Picasa, cloud-based photo service, which permits the storing, analysis, and sharing of photos among family and friends. This permits one to upload thousands of photos to Picasa and then analyze and sort them by use of the face recognition technology.

However, Google considered these privacy issues carefully when it released its Goggles application, which permits a person with a smartphone to take a photo and then initiate an Internet search of similar images. Goggles can be used for many images—buildings, product labels—but not for faces. Google declined to add that feature, which it could have done easily. It was determined that such a use would be dangerous, as it would permit a photo to be taken on the street and then used to identify, immediately, who that person was, where they lived, worked, or many more personal types of data accessible on the Web.

Discretion being the better part of valor, Google has not included face recognition in this Goggles application. Similar conversations are going on throughout corporate America, as the twin concerns of lawsuits and adverse public reactions weigh heavily on the minds of decision makers.

THE TREND CONTINUES

Yet it must be noted that there is a countertrend emerging of people who do not jealously guard their privacy. Smartphone apps that permit you to locate your friends based on GPS data from their devices, and also permit you to be found by them, are proliferating. Many of those enamored with social networking seem to be oblivious to concerns for privacy. Without a doubt, Max would warn his great-grandchildren against using these apps.

It is quite clear that with our increasing propensity for enhancing both security and efficiency, in these difficult economic times, more and more applications will be developed using biometric data. Again, these monitors and devices never sleep. Their usage will grow, in ways we cannot forecast at this time. There will be unintended consequences. That is the stuff of life. However, whether this trend is a positive one for mankind or not will be seen only in retrospect, years from now.

Max however would remain skeptical. Our world has changed and we must live in the present. But the world is still a hostile place—sometimes—and "they" are still out there.

NOTE

1. Lohr, S, "Computers That See You and Keep Watch Over You," *The New York Times*, Jan. 1, 2011, *http://www.nytimes.com/2011/01/02/science/02see.html*.