The Rise of Wearable and Smart Technology in the Workplace

by

Clement L. Tsao, Esq.
Cook & Logothetis, LLC
30 Garfield Pl Suite 540
Cincinnati, OH 45202
Ph: 513-287-6987
CTsao@econjustice.com

Kevin J. Haskins, Esq.
Preti, Flaherty, Beliveau & Pachios, LLP
One City Center
P.O. Box 9546
Portland, ME 04112-9546
Ph: (207) 791-3000
khaskins@preti.com

Brian D. Hall, Esq.
Porter Wright Morris & Arthur, LLP
41 S High St, Ste. 3100
Columbus, OH 43215
Ph: (614) 227-2287
BHall@porterwright.com

ABA National Symposium on Technology in Labor and Employment Law
Presented by the Technology in the Practice and Workplace Committee
April 5-7, 2017
Washington, D.C.
I. National Labor Relations Act Considerations by Clement L. Tsao

A. Surveillance

The National Labor Relations Board has long held that an employer engages in unlawful surveillance “when it surveils employees engaged in Section 7 activity by observing them in a way that is ‘out of the ordinary’ and therefore coercive.”

Aladdin Gaming, LLC, 345 NLRB 585, 585-86 (2005), petition for review denied, 515 F.3d 942 (9th Cir. 2008). See Allservice Plumbing & Maint., Inc., 2011 NLRB LEXIS 669, *41 (N.L.R.B. Dec. 1, 2011) (unlawful surveillance found where a supervisor went to a restaurant where a union meeting was being held, the supervisor stayed for thirty minutes, interrogated employees about their union activity, and had no other purpose beyond observing the union meeting). However, where an employer monitors protected activity but is able to show a legitimate business concern, the Board has permitted such activity to occur, and found there to be no violation of the Act. See Smithfield Foods, Inc., 346 NLRB 1225 (2006) (“[I]n light of the physical proximity of the handbilling to the [Employer’s] property and the temporal proximity of the previous trespassing incident, the [Employer’s] concern about a recurrence was reasonable and, therefore, the security guard’s redirection of the security camera was not unlawful.”).

It should not be difficult to imagine that the ability to track each employee’s precise location and physiological activity could have a chilling effect on protected concerted activity under the NLRA. Depending on the type of wearable technology

---

1 Cook & Logothetis, LLC, 30 Garfield Pl Suite 540, Cincinnati, OH 45202, 513-287-6987; CTsao@econjustice.com.

2 Under the National Labor Relations Act, workers have the right to engage in protected concerted activity. Section 7 of the Act provides in relevant part:

Employees shall have the right to self-organization, to form, join, or assist labor organizations, to bargain collectively through representatives of their own choosing, and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection . . .


3 Moreover, under the Board’s three-part test, “[i]ndicia of coerciveness include the duration of the observation, the employer’s distance from its employees while observing them, and whether the employer engaged in other coercive behavior during its observation.” Aladdin Gaming, LLC, supra at 586.

involved, employers could eventually, if not already, have the equivalent of a workplace ankle bracelet, i.e., GPS monitoring device, that could be used as a tool to monitor or interfere with protected concerted activity. For workplaces where there is a certified collective bargaining representative, wearable technology, or any form of a surveillance system, should be a mandatory subject of bargaining. See *Colgate-Palmolive Co.*, 323 NLRB 515, 515-16 (1997) (where the Board held that installation and use of surveillance cameras were mandatory subjects of bargaining). Given the likely chilling effect on protected concerted activity as well as in order to reduce the risk of unlawful surveillance, employers should establish and enforce policies for disabling wearable technology and collecting wearable data outside of working hours.5

B. Adopting a Collaborative Approach to Wearable Implementation

While the possibilities for wearable technology in the workplace may be enormous, so too are the litany of legal considerations that will inevitably arise. Perhaps a wise approach to take to avoid, or at least reduce, the challenges to wearable implementation would be to involve employees early on in – and at – each stage of the rollout process, which will hopefully result in the workforce buying into the use of wearable technology.6 The National Basketball Association (NBA) offers a good recent example of collaboration and player, or employee, input.

Late last year, NBA fans around the world breathed a sigh of relief when the NBA and the NBA Players Association (player’s union) reached an agreement for a new collective bargaining agreement, and avoided a possible strike or lockout. As part of the new agreement, the league and the player’s union agreed to form a joint advisory committee, made up of NBA officials and player representatives that will review and approve wearable devices for use by the players. While some teams had been using wearable devices in practices, players are currently not allowed to


wear such devices during games. How wearable devices and data are used in the future will be up to the new wearables committee.7

II. Privacy Considerations

A. (No) Expectation of Privacy?

For an increasing number of employees, expectation of privacy only truly begins when the workday ends, and ends when the workday begins. Many courts have found that employees do not have a reasonable expectation of privacy when employer-owned equipment or technology is involved, the employer has a legitimate business interest, and the intrusion occurs during normal work hours. See, e.g., Garrity v. John Hancock Mutual Life Insurance Co., 2002 U.S. Dist. LEXIS 8343 (D. Mass. May 7, 2002) (no reasonable expectation of privacy for emails sent on computer system owned by employer and where the employer has a legitimate business interest in protecting its employees from harassment); Thygeson v. U.S. Bancorp., 2004 U.S. Dist. LEXIS 18863 (D. Or. Sept. 15, 2004) (no reasonable expectation of privacy where employee used his employer’s computer and network for personal use, saved personal information in a location that was accessible by his employer, and the employee handbook prohibited personal use of the employer’s computer); Cunningham v. New York State Department of Labor, 997 N.E.2d 468 (N.Y. 2013) (unlawful and unreasonable search found where the employer “conducted a GPS search without making a reasonable effort to avoid tracking an employee outside of business hours”).8

In view of the trend towards deference to employer business interests, it seems inevitable that employee privacy claims involving wearable technology will only follow suit. For employee and privacy advocates, hopefully Congress and state legislatures can eventually prescribe boundaries regarding permissible data collecting and use at the workplace, and courts can continue to play the crucial role of balancing legitimate business interests with employee privacy.


B. Wearable Data, HIPAA, and Protected Health Information

The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule regulates and provides protections for the disclosure of Protected Health Information (PHI). See 45 C.F.R. §164.502. However, HIPAA’s obligations only apply to “covered entities,” which consist mainly of medical providers and their business associates. See 45 C.F.R. §160.103. However, as wearable technology becomes more prevalent in the workplace, employers will increasingly be collecting, using, and in possession of much of the same sensitive PHI as “covered entities,” but will be subject to none of HIPAA’s privacy requirements. Will employers be free to share, or even sell, that information to third parties? What happens to that information if the employer is bought out by another entity? Or if the employer is forced to close its operations? Declare bankruptcy? These kinds of considerations demonstrate the potential need for amendments to the HIPAA Privacy Rule or other updates to existing PHI protections.

III. Wearable Technology and Wage and Hour Litigation

Wearable technology data may be able to provide parties involved in wage and hour litigation the ability to significantly reduce, if not eliminate, the number of disputed factual issues. Overtime claims that would otherwise rely on the credibility and accuracy of witness testimony to determine if and when employees had been engaged in uncompensated work would likely settle upon the proper admission of reliable wearable data that could establish when the disputed work had been performed.

As more employers begin to use wearable devices in the workplace, employment attorneys should be prepared to request and produce relevant wearable data. Where such wearable data could be helpful towards complying with the Fair Labor Standards Act’s time and recordkeeping requirements (or resolving wage and hour disputes), employers may want to consider storing wearable data for the same period in which payroll records are kept. See 29 U.S.C. § 211 (“Every employer . . . shall make, keep, and preserve such records of the persons employed by him and of the wages, hours, and other conditions and practices of employment maintained by him . . . ”).

---


Moreover, once a party reasonably anticipates litigation, the duty to preserve evidence also applies to data generated or produced by wearable technology. See *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 218 (S.D.N.Y. 2003) (“Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a ‘litigation hold’ to ensure the preservation of relevant documents.”).
Wearable Technology and Implications for the ADA, GINA, and Health Privacy

Kevin J. Haskins, Esq.11

Wearable technology excels at providing data on health. The pedometer of yesterday has been relegated to the vintage dustbin: today’s fitness trackers, like those from Fitbit, Jawbone, Garmin, and Apple, can track not only heart rate and calories burned, but sleep patterns, walking patterns, sweat, diet, and a whole host of other health attributes when paired with mobile apps for tracking mood, fertility, and medication, to name just few.12 Although many of these devices are designed for the consumer market, they are becoming increasingly common in the workplace, often as part of employee wellness programs.13 Companies are also finding wearable devices useful for enhancing worker safety: devices for monitoring a worker’s hydration, temperature, movement, and external hazards are already available,14 and research is continuing into how to coordinate these tools into a “technological guardian angel” for workers.15 Not surprisingly, the proliferation of wearable technology in the workplace raises a number of legal issues.16 In particular, the intersection of wearable technology and health implicates issues under the Americans with Disabilities Act (“ADA”), the Genetic

11 Preti, Flaherty, Beliveau & Pachios, LLP, One City Center, P.O. Box 9546, Portland, ME 04112-9546, (207) 791-3000, khapskins@preti.com.
Information Nondiscrimination Act (“GINA”), and health privacy laws like the Health Insurance Portability and Accountability Act (“HIPAA”).

IV. ADA

A. Wearable technology and disability-related inquiries.

The ADA prohibits employers from administering medical examinations and other disability-related inquiries to current employees unless the examination or inquiry “is job-related and consistent with business necessity.” The EEOC’s enforcement guidance notes that a “medical examination” is any procedure or test “that seeks information about an individual’s physical or mental impairments or health.” That same guidance also defines a “disability-related inquiry” as any question that “is likely to elicit information about a disability.”

Because wearable devices are so adept at tracking health data and providing health analytics, there is a question about whether the use of these devices by employers implicates the ADA’s prohibition on medical examinations and disability-related inquiries. The multiple health parameters that wearable devices can track, and the granular nature of the information that they can provide, means that wearable technology can give end-users – both employers and employees alike – a veritable picture of an employee’s health. Even if a wearable device is not deployed by a company with the intent to conduct a medical examination, the information that the device yields still has the potential to elicit information about an employee’s disability. Wearable devices that monitor blood glucose or cardiac conditions, for example, could potentially be indicative of an employee’s diabetes or asthma.

Consequently, using wearable technology in the workplace does present a real risk under the ADA because it can provide an employer with employee-related health information that it would not otherwise have and that may relate to or disclose an underlying disability of an employee. Given this risk, companies deploying

---

19 Id.
wearable technology in the workplace should be prepared at a minimum to explain clearly to employees what information the technology collects, the limits on collection, and why the technology is job-related and consistent with business necessity.

There are two areas where the legal risks associated with wearable technology are arguably reduced under the ADA. The first relates to wearable technology used in connection with employee wellness programs, and the second relates to the use of wearable technology for safety-sensitive positions.

1. Wearable technology and employee wellness programs.

Employers are continuing to incorporate employee wellness programs into the workplace and, by some estimates, 40%-50% of them use health trackers as part of their programs. Part of the reason for this increase is the fact that the ADA specifically allows employers to conduct medical examinations and disability-related inquiries as a part of voluntary wellness programs. Consequently, even though the use of some wearable devices may constitute a medical examination or disability-related inquiry, the ADA provides an exception for that use in connection with voluntary wellness programs.

It is worth noting that, in January 2017, the EEOC’s new rules on workplace wellness programs went into effect. Although these rules do not directly address the use of wearable technology in connection with wellness programs, the rules do describe how such programs can comply with the ADA and GINA, and also remain consistent with the rules governing wellness programs under HIPAA.

One of the primary issues addressed in the new rules is the definition of “voluntary.” Although previous ADA regulations provided that employers could ask health-related questions and conduct medical examinations as part of a “voluntary” wellness program, the regulations did not define “voluntary” or address whether the offer of an incentive made a program involuntary. Now, the rules clarify that a wellness program that requires employees to answer disability-related questions or to undergo medical examinations may offer incentives of up to

22 See Haggin, supra note 15.
30 percent of the total cost for self-only coverage. This limit brings the ADA’s regulations in line with HIPAA, which applies the same incentive limit to health-contingent programs that require employees to achieve certain outcomes. In addition, for a wellness program to be considered voluntary, an employer may not require any employee to participate in the program, deny an employee access to health coverage if the employee chooses not to participate in the program, or take any adverse action based on an employee’s decision to not participate in the program.

The rules contain several other requirements that indirectly affect the use of wearable technology. For example, the rules require employers to provide a notice that clearly explains what medical information will be obtained from employees in a wellness program. The rules also require that wellness programs be “reasonably designed to promote health or prevent disease” – in other words, a wellness program must actually promote health and cannot include burdensome time requirements for participation, involve unreasonably intrusive procedures, or be used to shift insurance costs or to gain sensitive medical information that would otherwise be in violation of the law. In addition, the ADA also requires that employers make reasonable accommodations for employees with disabilities to participate in wellness programs. Consequently, if an employee’s disability or other condition precludes the use of wearable technology, then an employer should be prepared to consider reasonable accommodations that would allow the employee to participate in a wellness program without the technology.

In addition, the rules include two confidentiality provisions that are important to consider in connection with wearable technology. First, the rules provide that information from wellness programs may be disclosed to employers only in an aggregate form that does not disclose specific individuals. And second, the rules prohibit employers from requiring employees to agree to the sale of health information or the waiver of confidentiality as a condition for participating in a wellness program or receiving an incentive.

2. **Wearable technology and safety-sensitive positions.**

The ADA’s requirement that medical examinations and disability-related inquiries must be “job-related and consistent with business necessity” provides another potential caveat for the use of wearable technology. According to the EEOC, an inquiry meets the “job-related and consistent with business necessity” standard when an employer “has a reasonable belief, based on objective evidence, that: (1) an employee’s ability to perform essential job functions will be impaired by a
medical condition; or (2) an employee will pose a direct threat due to a medical condition.”

There are reasons to think that using wearable devices as an early warning system for employees in safety-sensitive positions could fall within this caveat. For example, for a forklift operator, a wearable device that measures enzymes in sweat and provides an alert whenever the operator becomes dehydrated or overly fatigued would presumably relate both to the operator’s ability to perform the essential job functions and whether the operator’s physical condition posed a direct threat of harm. And, the EEOC’s guidance suggests that medical inquiries may be warranted in certain circumstances where safety is at issue.

At the same time, the “job-related and consistent with business necessity” standard requires a reasonable belief, based on objective evidence, that an employee is impaired or poses a direct threat due to a medical condition. In other words, the standard arguably presumes that an observable medical condition already exists, the observation of which gives rise to reasonable belief that a medical inquiry is warranted due to the risk of impairment or a direct threat. Where wearable technology is used as an early warning system to detect a medical impairment before it even occurs, the elements of reasonable belief and objective evidence that would support the technology’s use are arguably absent.

In this area, much may depend on the particular data collected by wearable technology. Wearable devices that detect environmental hazards like carbon monoxide, or that provide geolocation data or serve to enhance mobility or sensory perception, for example, may not raise any ADA concerns because they do not track an employee’s medical condition and therefore are not likely to elicit any information about a disability. Rather, the use of those devices may raise other concerns, including issues around invasion of privacy and liability for accidents related to the use of wearable technology. The more that a wearable device provides continuous monitoring of an employee’s health condition, and the more detailed the information provided by the device, the greater the implications are under the ADA.

---


B. Wearable technology and discrimination.

Potential discrimination claims are another risk arising from the use of wearable technology in the workplace. The ADA prohibits discrimination against individuals on the basis of disability.\(^{28}\) The risk with wearable technology is that it can provide employers with a significant amount of employee-related health information that would not otherwise be available. Where the technology is used in connection with the performance of an employee’s job, an employee disciplined for job performance could conceivably claim that the real reason for the discipline is not a legitimate performance issue, but the employer’s discovery of a medical or health condition disclosed by the technology used by the employee to perform his or her job. Where wearable technology is used in connection with employee wellness programs, the risk is arguably lower because information collected about employees is often sent to a third-party provider, so that employers receive information only in the aggregate so as not to identify any particular employee. Even so, that “firewall” would not necessarily preclude the possibility of an employee claiming that an adverse action was based on a perceived disability, regardless of whether the information collected through wearable technology disclosed a disability, and regardless of whether the technology was used as part of an employee wellness plan.

Potential accommodation issues also exist with respect to wearable technology. As a general rule, it is employees who are required to initiate a discussion around the necessity for work accommodations due to a disability.\(^{29}\) However, the EEOC’s guidance on reasonable accommodations under the ADA suggests that an employer may have an obligation to initiate a discussion if it knows or has reason to know that an employee is experiencing workplace problems due to a disability.\(^{30}\) Consequently, in cases where wearable technology identifies that an employee is having problems with workplace performance, the information collected by the technology may, in some circumstances, require an employer to consider whether a physical condition of the employee is contributing to those problems.\(^{31}\)

Finally, it is worth noting that the EEOC has increased its focus on the use of “big data” in employment, \textit{i.e.} the use of algorithms and predictive analytics to evaluate

\(^{28}\) 42 U.S.C. § 12112(a).


\(^{30}\) Id.

\(^{31}\) See Haggin, \textit{supra} note 15.
large amounts of information collected about individuals. \(^{32}\) At a recent panel hosted by the EEOC that explored the use of big data in employment, the panel identified wearable devices used in connection with employee wellness plans as an area of concern, in part because little is known about how data analytic companies interpret data collected from wearables, and the data provided by such devices can oftentimes be unreliable. \(^{33}\) Given the EEOC’s interest in “big data” and how it is used by employers to make employment decisions, it is likely that the EEOC will be interested in how the use of wearable technology in the workplace contributes to this emerging issue.

V. GINA

Similar to the ADA, the Genetic Information Nondiscrimination Act prohibits discrimination in employment on the basis of genetic information. \(^{34}\) The law defines “genetic information” as including, among other things, information about an individual’s genetic tests, genetic tests of that individual’s family members, and the manifestation of disease or disorder in family members of the individual, i.e. family medical history. \(^{35}\) Among other protections, the GINA makes it unlawful to “request, require, or purchase genetic information of an individual or family member of the individual.” \(^{36}\)

For wearable technology, then, the GINA raises many of the same risks and concerns as the ADA. If an employee is required to wear a device that collects genetic information or, as a requirement to using such a device an employee is required to provide that information or other information about his or her family’s medical history, there is a risk that the wearable technology would amount to an unlawful request for genetic information. Depending on the information collected by a wearable device, the GINA also presents similar risks for potential discrimination claims.

The GINA does provide an exception to the general prohibition against requesting, requiring, or purchasing genetic information. That exception applies where employers offer voluntary health or genetic services to employees or their family

---


\(^{34}\) 42 U.S.C. § 2000ff.

\(^{35}\) 29 C.F.R. § 1635.3(c)(1).

\(^{36}\) 29 C.F.R. 1635.8(a).
members as part of a wellness program.\textsuperscript{37} Many of the same requirements contained in the new rules issued by the EEOC, which relate to the ADA and wellness programs and are discussed above, apply equally to the GINA.\textsuperscript{38} For that reason, much of the discussion above relating to wearable technology and wellness plans under the ADA is equally relevant to wellness plans under the GINA.

Notably, there is a bill currently pending in the House of Representatives, H.R. 1313, that would make the GINA inapplicable to workplace wellness programs.\textsuperscript{39} Under the proposed bill, employers would arguably be able to “upcharge” employees who choose not to provide genetic information as part of a voluntary wellness program. The fate of this bill, however, remains uncertain.

VI. Health Privacy

Wearable technology that collects health-related information from employees also implicates the Health Insurance Portability and Accountability Act. HIPAA sets out national standards for protecting individually identifiable health information – or protected health information, PHI – held by “covered entities” and their business associates.\textsuperscript{40} These standards are incorporated into the HIPAA Privacy Rule, which sets forth the circumstances under which PHI may be disclosed by covered entities; the Security Rule, which sets forth the procedures that covered entities must follow to ensure the protection of PHI; and the Breach Notification Rule, which requires covered entities and their business associates to provide notification of breaches of unsecured PHI.

However, HIPAA does not apply to employers in their capacity as employers. Rather, HIPAA applies only to “covered entities” and their business associates. Under HIPAA, a “covered entity” is defined as a health plan, a health care clearinghouses, and most health care providers.\textsuperscript{41} For many employers, then, HIPAA obligations do not apply, which means wearable devices that are used in those workplaces and that collect health-related information from employees are not subject to HIPAA either.

\textsuperscript{37} 29 C.F.R. § 1635.8(b)(2).
\textsuperscript{40} See 45 C.F.R. Parts 160, 162, and 164.
\textsuperscript{41} 45 C.F.R. § 160.103.
As for workplace wellness programs, whether the HIPAA rules apply depends on whether the program is independently offered by an employer (not a covered entity), or whether it is offered as part of a health plan. If the program is directly offered by an employer outside of a health plan, then HIPAA would not apply and any information collected from employees – including information collected from wearable devices – would not be protected. If, however, a wellness program is offered as part of a group health plan, then any PHI collected from participants in the program would be protected by the HIPAA rules.\(^{42}\)

Interestingly, it appears that at least some wearable device manufacturers may be adopting a conservative approach and are designing their products to be HIPAA-compliant even though, in many workplaces, it is not technically necessary to do so. Fitbit, for example, announced in September 2015 that its devices were HIPAA-compliant, enabling the company to further integrate its offerings with HIPAA-covered entities.\(^{43}\) In this quickly evolving area of wearable technology and employment, that conservative approach may be the best one to take not just for wearable manufactures, but employers and employees as well.


The rise of smart and wearable technology in the workplace creates new questions for employers to consider in their efforts to protect their trade secret information. Consider, for instance, whether the proliferation of smartphone applications such as Snapchat, which permit employees to create self-destructing photos or videos or applications such as Facebook Live and Periscope, which permit live video broadcasting, create new risks of trade secret disclosure. Will adoption of the Internet of Things in the workplace, which permits various smart devices to “talk” to each other, create more data transfers that are subject to hacking? Will the use of augmented reality through smart glasses put warehouse inventory levels or designers’ 3D design drawings at greater risk for disclosure. Similarly, employers will want to guard against miscreant employees’ use of various means that are now available to permit recording devices and flash drives and other mobile storage media to be concealed in items such as jewelry.

A. Trade Secret Definition

Setting aside for a moment the risk of disclosure, let’s first consider where the trade secrets may lie in this new technology. Under the Uniform Trade Secrets Act (UTSA), which as of March 2017 has been adopted in some form by every state other than New York and Massachusetts, a “trade secret” is defined as information that (1) “derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use;” and (2) is “the subject of efforts that are reasonable under the circumstances to maintain its secrecy.” The federal Defend Trade Secrets Act defines a “trade secret” as “all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if: (A) the information derives independent
economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by another person who can obtain economic value from the disclosure or use of the information; and (B) the owner thereof has taken reasonable measures to keep such information secret.

1. Derives Economic Value Through Secrecy

For employers, the three likeliest sources of trade secret information arising out of the implementation of any smart or wearable technology program in the workplace would seem to be: (1) the steps taken to customize the technology for use in the employer’s workplace; (2) the data that the employer collects from the technology; and (3) the analysis of that data in order to implement workplace policy and procedure changes. Each of these sources would certainly create economic value to the employer if they are kept a secret from others.

For instance, some employers are testing or even using wearable badges that measure such things as location monitors, motion detectors and voice measurement sensors that permit the employers to identify patterns as it relates to face to face interactions between co-workers and with customers. Such data likely would permit the employer to measure the various interactions over a period of time and to identify the data patterns associated with the most and least successful work groups and/or individual employees. The customization of the technology program to the employer’s workplace – e.g., which groups the employer chose to measure, in which locations of the workplace, which variables it chose to measure and which to ignore, etc. – all would be valuable information to competitors if known. Similarly, and probably more importantly, the data obtained from the badges, how that data is analyzed, the workplace decisions made based on that data, and the

46 See e.g. Metallurgical Indus. v. Fourtek, Inc., 790 F.2d 1195, 1202 (5th Cir. 1986) (“[A] trade secret can exist in a combination of characteristics and components[,] each of which, by itself, is in the public domain, but the unified process, [the] design and operation of which in unique combination[] affords a competitive advantage, is a protected trade secret.”); Penalty Kick Mgmt. Ltd. v. Coca Cola Co., 318 F.3d 1284, 1291 (11th Cir. 2003) (“[E]ven if all of the information is publicly available, a unique combination of that information which adds value to the information also may qualify as a trade secret.”); Naturalawn of Am., Inc. v. West Group, LLC, 484 F. Supp. 2d 392, 399 (D. Md. 2007) (Software that is publicly available in its basic form may still constitute a trade secret where the plaintiff has customized and enhanced it to make it unique.)
47 Decision Insights, Inc. v. Sentia Group, Inc., 2009 U.S. App. LEXIS 2654 (4th Cir. 2009) (Remanding case to the district court for a determination of whether the plaintiff’s software compilation constitutes a trade secret under Virginia law.); Isc-Bunker Ramo Corp. v. Atech, Inc., 765 F. Supp. 1310 (N.D. Ill. 1990) (Data compilation constitutes trade secret under Illinois law even if the plaintiff did not develop the data itself.)
48 See e.g. Glaxo Inc. v. Novopharm Ltd., 931 F. Supp. 1280, 1299 (E.D.N.C. 1996) (noting that a trade secret can consist of “data that would give a person skilled in the art a competitive advantage he might not otherwise enjoy but for the knowledge gleaned from the owner’s research investment”); P&G v. Stoneham, 140 Ohio App. 3d 260 (2000) (enforcing non-compete agreement to protect trade secrets including in part marketing data analysis.)
successes and/or failures achieved based on that analysis presumably all provide a substantial competitive advantage over competitors that have not tried the badges.

2. Reasonable Security Efforts

 Fortunately, while technology may be evolving and thereby creating new forms of trade secret information, most of the tried and true methods for securing that information still should work. Under the Uniform Trade Secret Act (“UTSA”) adopted by most states and the relatively new federal Defend Trade Secrets Act (“DTSA”), businesses are required to use reasonable efforts to maintain the secrecy of any information claimed to be a trade secret. Such efforts typically include:

a. Name / Label Files According to Sensitivity: It is a worthwhile endeavor to create a data map of all of its information. A data map would identify all storage devices and containers, what data reside on those devices and in those containers, and where that data travels internally and externally. Then, and this probably goes without saying, identify and label all files, both hard copy and electronic, based on their sensitivity. Finally, establish appropriate handling procedures (such as copying restrictions, requiring encryption in transit, etc.) for these files.49

b. Employee Confidentiality and Non-Competition Agreements: Obtain these agreements upon the hiring of the employees to avoid issues of consideration. Ensure that they are broad enough to protect trade secrets but not so broad that their enforceability is subject to attack. Supplement these agreements with employee handbook provisions and job descriptions that emphasize the importance of maintaining confidentiality of data with which the employees work. Non-competition agreements should obligate the departing employee to notify the employer of any new employment obtained during the restricted period and to provide a copy of the agreement to any prospective employers.50

49 See e.g., Mattel, Inc. v. MGA Entm’t Inc. & Consol Consol. Actions, 782 F. Supp. 2d 911, 959; 2010 U.S. Dist LEXIS 136922 at *71 (C.D. Cal. 2010) (“[A]n employer’s failure to mark documents as confidential or trade secret precludes in many cases trade secret protection for those materials.”). See also Diamond Power Int’l, Inc. v. Davidson, 540 F. Supp. 2d 1322, 1335; 2007 U.S. Dist. LEXIS 73032 at *26 (N.D. Ga. 2007) (denying judgment as a matter of law on claim alleging misappropriation of trade secrets based on a hardware book file because, Plaintiff, among other things, did not label the file confidential or otherwise communicate the confidentiality of the file directly to employees or direct employees to maintain the secrecy of the file).

50 See e.g. Del. Elevator, Inc. v. Williams, 2011 Del. Ch. LEXIS 47 (2011) (finding that the plaintiff made reasonable efforts to keep its customer list confidential by having its sales personnel and senior management
c. Third Party Due Diligence and Non-Disclosure Agreements: To the extent that employers need to work in cooperation with other companies in, for instance, planning and implementing a smart or wearable device program or analyzing the data derived from it, they will want to ensure that they do appropriate due diligence on the companies with which they intend to work and enter into non-disclosure agreements with them.51

d. Limit and Monitor Access: Access to trade secret information should be limited to a need-to-know basis. Indeed, depending on the value of the trade secret and the ability to effectively do so, it might be appropriate to ensure that no employee knows all aspects of the trade secret. Employee access should be monitored to ensure that no inappropriate access occurs and to take steps to revise any procedures that need tightening. Processes should also be put in place to terminate access whenever the employee’s need for access ends, such as due to an employee’s change in assignment or separation.52 Finally, while our microwave ovens may not really be spying on us53, employers should remain vigilant against new technologies that permit employees to conceal flash drives and other portable media devices in jewelry and other discrete hiding places.54

e. Employee and Vendor Background Checks: Periodic background checks (in accordance with the Fair Credit Reporting Act and analogous state laws and EEOC guidance) should be required for all applicants and employees (and vendors’ employees) who will be working in sensitive areas, or who will have access to confidential information.55

employees enter into non-competition agreements and therefore finding that the customer list thus qualified as a trade secret under Maryland law.)

51 See e.g. Rockwell Graphic Systems, Inc. v. DEV Industries, Inc., 925 F.2d 174 (noting as a factor in denying summary judgment against the plaintiff, *inter alia*, that vendors who accessed proprietary drawings were required to sign confidentiality agreements.)

52 RoundPoint Mortg. Co. v. Florez, 2016 NCBC 17 (N.C. Superior Court, 2016) (favorably noting that employer computer systems are only accessible internally by using usernames and passwords and are only accessible outside of the office with a username, password, and remote-connection software; that certain files are accessible only to specified employees through restricted shared network drives or by email to specified individuals who have a legitimate business need for the information; and that access to company settings and customizations to proprietary software is limited to administrators, and administrator status is tightly controlled.)


55 See e.g. Lexjet, LLC v. Big Dog Media Solutions, LLC, 2014 U.S. Dist. LEXIS 180393 (M.D. Fla. 2014) (noting that former employees were not subjected to background checks in decision denying preliminary injunction in trade secret misappropriation case.)
f. Employment Policies Restricting Photos and Recording: With the rapid rise of smart technology that enables workers to photograph, video and broadcast from almost anywhere at any time and at very high resolution, employers should restrict the use of such technology in sensitive areas of its facilities and when working with specific trade secret information. Don’t forget about audio. Prohibit audio recording of any meetings at which trade secret information is discussed. Any audio, photography or video restrictions should be narrowly tailored to avoid issues under the National Labor Relations Act.56

g. Trade Secret Focused Exit Interviews: The exit interview is an employer’s last chance to remind employees of their contractual obligations regarding competition and confidentiality as well as under trade secret laws. Departing employees should be given a checklist of information that the employer considers to be trade secret in nature to initial. The employer should also ask the departing employee to identify any new employment and document the answer given (or the refusal to answer.) The exit interview also provides the final reminder to ensure that the employee’s computer and other access has been terminated, to identify and review any suspicious computer and/or physical access leading up to the last date of work, to obtain the return of company devices, keys and other means for accessing data, and to ensure that any company information kept on an employee’s owned devices that have been connected to the company network is wiped and removed from any cloud services.57

VIII. E-DISCOVERY

Implementation of any smart or wearable technology program in the workplace will raise many litigation hold and e-discovery issues for employers. Although we are only scratching the surface of issues raised, we will focus on how new technologies are impacting litigant obligations as it relates to implementing litigation holds.

56 See e.g., Whole Foods Market, Inc., 363 NLRB No. 87 (2015) (determining that company’s ban on workplace recordings violated employees’ Section 7 rights) but see Flagstaff Medical Center, 357 NLRB No. 65 (2011) (upholding company’s no-recording ban in hospital because “privacy interests of hospital patients are weighty,” and the hospital had a “significant interest in preventing the wrongful disclosure of individually identifiable health information.”

57 See e.g., Tyson Foods, Inc. v. ConAgra, Inc., 349 Ark. 469 (2002) (in which the court put the burden on the plaintiff employer to clearly identify the information it considered to be a trade secret and noted that the employer could have used an exit interview to advise the departing employee what it considered to be proprietary.)
A. Ephemeral Messaging Apps

New ephemeral messaging apps are coming on the market all the time. These are messaging apps, such as Snapchat, Confide, Wickr, and Cyber Dust, that boast that they self-delete upon receipt and theoretically leave no trace afterward. Many of them have been developed specifically for a business environment. For instance, Mark Cuban, the billionaire who apparently is among the financial backers of Cyber Dust, reportedly described the app as an alternative to face to face communication, which means that “Nothing is discoverable.”

Obviously, such apps can create litigation hold and e-discovery issues. From a litigation hold perspective, a litigant can only preserve what is in its possession, custody or control, so there obviously can be no obligation to preserve what does not exist. But, does the reasonable anticipation of litigation bring with it the obligation to cease using messaging apps for communications related to the subject matter of the anticipated litigation when the organization or individual knows the communications will self-delete upon receipt?

From the perspective of attempting to discover communications made using ephemeral messaging apps, the litigant would be wise to serve interrogatories designed to understand the extent and nature of the use of such apps by the organization or the individual on the other side, but then the question quickly will become one of cost of proportionality. Rule 26(b)(2) of the Federal Rules of Civil Procedure permits a court to limit “the frequency or extent of discovery” where “the burden or expense of the proposed discovery outweighs its likely benefit, considering the needs of the case, the parties’ resources, the importance of the issues at stake in the action and the importance of the discovery in resolving the issues.” Absent a substantial showing that communications using ephemeral messaging apps will be highly relevant to the subject matter of the litigation and that metadata (if not content) related to those communications will be recoverable, the federal rule on proportionality likely will result in a decision to forego such discovery. Instead, most litigants will prefer to rely on the inference that the user is attempting to hide something that is created by knowledge of the use of the app in the first place.

---

58 Many mobile apps that were capable (or at least claimed to be capable) of saving Snapchat photos, video and text have been rendered useless by Snapchat updates to the app. To this date, however, one still can find on the internet many other, albeit more complicated, methods for making the saves.

B. Information Stored In The Cloud

Data obtained through wearable and other smart technology likely will be stored in the cloud in addition to whatever data may be stored on the device itself. In employment litigation, it is relatively easy to contemplate the circumstances under which data stored in the cloud might be subject to discovery. For instance, there will be many cases in which the employer relies on data stored in the cloud to support an employment decision and questions will arise as to who has access to the data. There will also be cases where employee data will be stored in their personal cloud accounts. E-discovery obligations cannot be avoided simply by contracting with a third-party provider to store data in the cloud. Indeed, a business can face a bigger challenge meeting its obligations within a cloud environment because it does not have complete control over what happens to data stored with a cloud provider.

Brown v. Tellermate Holdings Ltd., 2014 U.S. Dist. LEXIS 90123 (S.D. Ohio 2014) provides a prime example of this type of challenge. In Brown, plaintiffs brought an action alleging that Tellermate had terminated their employment due to their age. During discovery, Plaintiffs, as part of their effort to show that their sales performance was comparable to or superior to other younger Tellermate employees, who had not been terminated, asked Tellermate to produce from salesforce.com “reports” both for themselves and for a number of other employees whom they named in their document request. Tellermate resisted this discovery request on the grounds that: it “does not maintain salesforce.com information in hard copy format, …cannot print out accurate historical records from salesforce.com, .... [and] “discovery of salesforce.com information should be directed to salesforce.com, not Tellermate.” Each of these grounds proved to be erroneous as was easily determinable in most cases by even a cursory reading of the service agreement.

Then in opposition to a motion to compel discovery, Tellermate represented:

- “Tellermate is contractually prohibited from providing salesforce.com information - including information Tellermate inputs into it - to third parties” (an untrue statement);

---

“In addition to the contractual prohibition on Tellermate providing salesforce.com information, Tellermate cannot provide the information Plaintiffs seek in any event” (also an untrue statement); and
- “Tellermate can only access the salesforce.com database in real time; Tellermate cannot access historical salesforce.com data” (yet another untrue statement).”

The parentheticals quoted above were from the Magistrate Judge’s opinion, which obviously did not bode well for Tellermate or its counsel. By the time Tellermate’s counsel made a request for the data maintained on salesforce.com, the data had been subject to updating and alteration for two and a half years, meaning that there was no way of knowing whether the data was reliable.

Noting that Tellermate knew from the outset that its termination of the [plaintiffs] was premised on their allegedly inadequate sales performance, the Magistrate concluded that the failure to preserve the integrity of the salesforce.com data was sanctionable and issued an order precluding Tellermate from presenting or relying on any performance-based criteria in support of its argument that it had a legitimate non-discriminatory reason for terminating the plaintiffs’ employment, since it had essentially prevented them from learning how their performance compared to other sales representatives at the time.

On objections to the district judge, Tellermate’s new counsel was able to convince the court that the sanction recommended by the Magistrate exceeded the prejudice to the plaintiffs. Brown v. Tellermate Holdings Ltd., 2015 U.S. Dist. LEXIS 105263 (S.D. Ohio 2015). Nevertheless, the court still sanctioned Tellermate as follows:

1. Defendant Tellermate shall not be permitted to introduce salesforce.com records as evidence at trial or refer to those records at trial;
2. Defendant Tellermate is precluded from asserting that the Plaintiffs’ use or non-use of the salesforce.com application was in any way deficient or that it justified their termination;
3. If evidence at trial raises any contested issue about the sales conduct of the Plaintiffs or any other Tellermate salesperson, and the Plaintiffs show that missing salesforce.com data would corroborate their position, then the Court will give the jury an adverse inference instruction appropriate for the circumstances; and
4. The Plaintiffs will be permitted to testify as to what the salesforce.com records would have shown had they been properly preserved. Defendant Tellermate may rebut this testimony only through independent evidence, and not the salesforce.com records.”

Similarly, in Selectica Inc. v. Novatus, Inc., 2015 U.S. Dist. LEXIS 30460 (M.D. Fla. 2015), a trade secrets misappropriation case, the court held that Novatus, which had hired Selectica’s employee had a duty to preserve Selectica documents that the employee had pushed to his personal Box.com account. Concluding that Novatus had control over its employee’s documents, the court concluded that the company was obligated to have ensured that the employee preserved the documents he stored in the cloud.

C. Information Stored On Employee-Owned Devices

Federal courts are divided on when and how a party seeking discovery can access data stored on an employee’s personal device. In Alter v. Rocky Point Sch. Dist., 2014 U.S. Dist. LEXIS 141020, (E.D.N.Y. Sept. 30, 2014), the plaintiff alleged that she was subjected to a hostile work environment based on her gender and then retaliated against once she complained. During the course of the litigation, the plaintiff filed a motion to compel discovery and for sanctions alleging that the school district failed to implement a proper litigation hold, which resulted in spoliation of evidence. Among the items of discovery that the plaintiff sought but were unavailable were documents stored on school district employees’ personal computers that were not available to produce. The court stated that the school district was obligated to have identified key employees with relevant information and then to have instructed them to preserve any relevant documents “whatever devices contained the information,” including personal computers. See also In Re Pradaxa (Dabigatran Etxilate) Products Liability Litigation, MDL No. 2385 (S.D. Ill. Dec. 9, 2013) (in which the court held that business-related text messages on employees’ personal cell phones should have been preserved pursuant to a litigation hold). Cf. In re Boehringer Ingelheim Pharms., Inc., 745 F.3d 216 (7th Cir. 2014) (in which the court upheld sanctions where the defendant failed to preserve employee text messages on company-owned cell phones); Stinson v. City of New York, 2016 U.S. Dist. LEXIS 868 (in which the court held that city police department-issued cell phones were in the city’s possession, custody and control and therefore “were subject to the same preservation obligation as the City’s other ESI.”).

In Cotton v. Costco Wholesale Corp., 2013 U.S. Dist. LEXIS 103369 (D. Kan. 2013), a Title VII race discrimination case, however, the court refused to order the
defendant to produce text messages sent or received by two employees on their personal devices that mentioned the plaintiff. In reaching this conclusion, the court noted that there was no suggestion from the plaintiff “that Costco issued the cell phones to these employees, that the employees used the cell phones for any work-related purpose, or that Costco otherwise has any legal right to obtain employee text messages on demand.” Accordingly, the court noted that “Costco does not likely have within its possession, custody, or control text messages sent or received by these individuals on their personal cell phones” and therefore denied the plaintiff’s motion to compel discovery.