Bloomberg BNA

Privacy and Security Law Report®

The Brave New World of Wearables in the Workplace: Privacy and Data Security Concerns for Employers

BY PHILIP GORDON AND ZOE ARGENTO

With the projected growth of wearable technology into a $20-billion-plus industry in the next five years, employers can expect that employees increasingly will work clad in an array of sensors and computing devices. Employees already have effectively worn computers in the workplace in the form of personal mobile devices in a pocket or handbag for nearly a decade. Wearables, however, take ''personal computing'' to the next level, creating unprecedented potential not only for efficiency but also for intrusion into the privacy of others and for compromise of the data that wearables can collect. This article considers these privacy and data security challenges for employers as the new world of wearables in the workplace approaches.

I. Wearables in the Marketplace: Examples of Personal and Business Use

At a high level, wearable technology consists of four elements: sensors, a display, computing architecture and the capacity to operate in an essentially hands-free manner. These technologies integrate into users' activities in a qualitatively different way than smartphones and other personal mobile devices. Rather than functioning as separate devices, wearables are an extension of the wearer.

The most popular consumer wearables fall into four main functional categories: fitness trackers, health trackers, ready-reference devices and history-recording devices.

- **Fitness trackers**: Fitness trackers track different aspects of the wearer's exercise patterns. One popular device, the Fitbit, fits discretely around the user's wrist and records the number of steps the user takes. Fitness trackers now hold the largest market share among consumer wearables.
- **Health trackers**: These wearables help individuals monitor specific health conditions. For example, the QardioCore, a strap worn around the chest, functions as a personal electrocardiogram by continually monitoring the heart's electrical activity.
- **Ready-reference devices**: These devices are more like smartphones in that they provide access to the world of online information. The wearable versions, however, are more accessible. The Pebble, currently the most popular smart watch, provides alerts for text messages, e-mails and appointments and at-a-glance access to a range of information, including location, restaurant reviews and weather reports.
- **History-recording devices**: This wearable technology records the wearer's experiences. For example, Google Glass can stream what the wearer sees in real time to anyone with an Internet connection. The neurocam, another eyewear device, detects the wearer's interest by analyzing her brain activity and then takes a video of whatever piqued her interest.

Consumer wearables have rapidly entered the mainstream. According to a survey by PricewaterhouseCoopers LLP, one in five American adults owned a wearable device in 2014.[1] This number is projected to increase substantially in the next five years.

Philip Gordon is a shareholder in Littler Mendelson PC's Denver office and chair of the firm's Privacy and Data Protection Practice Group.

Zoe Argento is an associate in Littler Mendelson's Denver office, where she counsels clients on all aspects of workplace privacy and information security.

[1] PricewaterhouseCoopers LLP, The Wearable Future (2014) [hereinafter Wearable Future], *available at* http://www.pwc.com/us/en/industry/entertainment-media/

 ISSN 1538-3423

Although the consumer market has, to date, been the primary driver of developments in wearable technology, businesses have begun to adopt wearables in at least five major categories: performance enhancers, performance managers, seamless reference, location tracking and authentication.

- **Performance enhancers**: Performance enhancers augment the physical capabilities of the worker. For example, Evena Medical has developed eyewear called Eyes-On Glasses that helps nurses find a vein on a patient using spectral imaging.
- **Performance managers**: Performance management devices help wearers sustain a high level of performance by monitoring physical indications. For a desk worker, this might simply mean monitoring posture to reduce the risk of ergonomic-related injuries, such as back strain. The LUMO-Back device, for example, straps around the waist and buzzes when the wearer's posture slips. For workers in more demanding conditions, say a technician working in a hot engine room, devices like the Electrozyme can detect electrolyte and hydration levels to help a worker determine when she needs to rehydrate or take a break. Unlike the performance enhancers, which provide the wearer with new physical capabilities such as the ability to see a vein under the skin, the performance managers focus on helping the wearer maintain his or her existing capabilities.
- **Seamless reference**: While the performance enhancer and performance manager categories provide more information about the user's physical environment, seamless reference devices provide immediate access to information and analysis from beyond the user's vicinity. A technician wearing an eyeglass device called XOEye, for example, can stream what she sees to an expert in another location. The expert can then help the technician diagnose an equipment failure and guide the technician's repair.
- **Location tracking**: Location tracking devices record employees' movements on the job. These wearables have the potential to help companies redesign spaces and reorganize work for better performance and cost-effectiveness. Such a device could, for example, help a transportation company determine how it may most efficiently position workers on a loading dock.
- **Authentication**: Authentication devices authenticate the wearer with unique biomarkers, thereby potentially reducing the risk of identity theft. As an example, the Bionym Nymi uses an individual's cardiac rhythm to authenticate his or her identity, unlocking electronic devices as the wearer approaches them.

As these examples illustrate, wearables have the potential not only to increase employees' efficiency, but also to enhance their well-being and safety.

publications/consumer-intelligence-series/assets/PWC-CIS-Wearable-future.pdf.

II. Legal Issues: Privacy and Data Security Risks

For many businesses, the need to maintain or improve competitiveness will create an imperative for the adoption of wearables. Regardless of whether they adopt wearables themselves, however, many employers will have to grapple with issues presented by wearable technology as increasing numbers of employees wear these devices in the workplace.

Wearables pose a wide range of privacy and data security risks for employers.

Wearables pose a wide range of privacy and data security risks for employers. The legal issues depend on three major factors:

- whether the employer or the employee owns the wearable;
- whether the wearable's sensors collect information about the wearer or about others; and
- whether the wearable is used in the U.S. or overseas.

We address the legal issues associated with each factor in turn.

A. Employer-Provided Wearables

A growing number of companies provide wearables to their workers. The principal privacy risk in these situations relates to information collected by these devices about individual workers, whether the wearer herself or co-workers. As discussed below, and depending on the category of information, simply collecting the information could lead to legal liability. Storing and using the information can present additional risks.

1. Information Collected by the Wearable About the Wearer

a) Health Information

Employers generally are prohibited from using employer-provided wearables, such as performance managers or health trackers, to collect health information about employees. However, they might be able to use health trackers as part of a voluntary wellness program.

The Americans with Disabilities Act (ADA) generally prohibits employers from making disability-related inquiries of current employees unless the inquiry is job related and consistent with business necessity.[2] In its ''Enforcement Guidance on Pre-Employment Disability-Related Inquiries,'' the Equal Employment Opportunity Commisson (EEOC) interpreted this prohibition to extend to an inquiry that is likely to elicit information about a disability even though the inquiry does not on its face ask about a disability.[3] For example, an employer's review of data from a worker's blood pressure

[2] 42 U.S.C. § 12112(d)(4).

[3] EEOC, *Enforcement Guidance on Pre-Employment Disability-Related Inquiries*, EEOC Notice No. 915.002, *avail-*

  PVLR ISSN 1538-3423

monitor likely would fall under the EEOC's interpretation of a disability-related inquiry. Blood pressure could indicate a number of disabilities, such as an increased susceptibility to strokes, heart failure and aneurysms. Notably, there is no consent exception to the ADA's general prohibition on disability-related inquiries.[4] Consequently, outside the context of a voluntary wellness program (discussed below), it would be risky for employers to even ask employees to volunteer to wear a health tracker or a performance enhancer that would permit the employer to collect health information about the employee.

The ADA also prohibits employers from making employment decisions based on disabilities unrelated to job function.[5] Consequently, even reviewing apparently innocuous information that might not be considered a disability-related inquiry under the ADA, such as a Fitbit report on the number of steps an employee takes, potentially could lead to litigation for an employer. For example, an employee might log a low number of steps per day due to a heart condition. If the employer discharged the employee after reviewing the Fitbit record, the employee might allege that the employer terminated the employee because of a disability or perceived disability, even if the employer actually terminated the employee for a legitimate reason.

Before integrating health-tracking wearables into their wellness programs, employers should carefully analyze the legal requirements surrounding such programs.

The ADA does allow employers to conduct voluntary medical examinations as part of an employee health program, such as a voluntary wellness program.[6] Many employers use wellness programs, such as wellness fairs, incentives to join gyms and smoking cessation programs, to enhance employee well-being and to reduce health benefit costs. These programs are popular. According to a 2012 survey by ADP LLC, nearly 80 percent of companies with more than 1,000 employees provided some type of wellness program.[7]

Health-tracking wearables are a natural fit for wellness programs. Real-time access to information about their own bodies and health could help employees make better health choices. By providing a constant reminder, a blood pressure monitor might, for example, encourage an employee to take the daily steps necessary to reduce high blood pressure. Seventy percent of consumers say they would wear employer-provided wearable technology that anonymously pools their data in exchange for lower insurance premiums.[8] Some employers, such as Bates College, VISTA Staffing Solutions and Appirio, have already incorporated wearables into their wellness programs.[9]

Before integrating health-tracking wearables into their wellness programs, however, employers should carefully analyze the legal requirements surrounding such programs. While the EEOC interpretation acknowledges that the ADA allows for voluntary wellness programs, the agency emphasizes that such programs must be truly ''voluntary.''[10] To be ''voluntary,'' employees must neither be required to participate nor penalized for nonparticipation in the wellness program.[11] The EEOC has recently stepped up its enforcement of this point. In 2014, the EEOC filed three lawsuits against companies alleging that their employee wellness programs were insufficiently voluntary.[12]

Employers that consider offering employees an incentive, such as a reduction in the employee's contribution to health benefit costs, to don a wearable in conjunction with a wellness program should beware. The EEOC has not yet taken a position on whether it would defeat the voluntary nature of a wellness program to offer an incentive to employees who participate, but not to those who opt out of the wellness program.[13] The EEOC has announced it will provide more guidance on this point in February 2015.[14]

Even if the wellness program is sufficiently voluntary and an employee consents to participate, any information collected that could reveal a disability must be handled in accordance with strict requirements imposed by the ADA. Employers must:

- maintain such information separately from the employee's personnel file;
- provide access only to human resources or benefits employees with a need to know and not to supervisors or other employment decision-makers;
- not use the information for employment purposes; and

able at http://www.eeoc.gov/policy/docs/waiver.html; ADA Manual (BNA) 70:1103 (1995).

[4] 42 U.S.C. § 12112.

[5] *Id.* at § 12112(a).

[6] *Id.* at § 12112(d)(4)(B).

[7] ADP, *Why You Should Care About Wellness Programs* (2012) at 15, *available at* http://www.adp.com/tools-and-resources/adp-research-institute/research-and-trends/~/media/RI/whitepapers/Why-You-Should-Care-About-Wellness-Programs.ashx.

[8] Wearable Future, *supra* note 1.

[9] James A. Martin, *Pros and Cons of Using Fitness Trackers for Employee Wellness*, CIO, Mar. 24, 2014, *available at* http://www.cio.com/article/2377723/it-strategy/pros-and-cons-of-using-fitness-trackers-for-employee-wellness.html.

[10] EEOC, *EEOC Enforcement Guidance on Disability-Related Inquiries and Medical Examinations of Employees Under the Americans with Disabilities Act (ADA)*, EEOC Notice No. 915.002, at Q&A 22 (July 27, 2000), *available at* http://www.eeoc.gov/policy/docs/guidance-inquiries.html.

[11] *Id.*

[12] Petition for a Temporary Restraining Order and Preliminary Injunction, EEOC v. Honeywell Int'l, Inc., No. 0:14-cv-04517-ADM-TNL (D. Minn. Oct. 27, 2014); Complaint, EEOC v. Flambeau, Inc., No. 3:13-cv-00638 (W.D. Wis. Sept. 30, 2014); Complaint, EEOC v. Orion Energy Systems, No. 1:14-cv-01019 (E.D. Wis. Aug. 20, 2014) (13 PVLR 2156, 12/22/14).

[13] EEOC Informal Discussion Letter, *ADA: Voluntary Wellness Programs & Reasonable Accommodation Obligations*, Jan. 19, 2013, *available at* http://www.eeoc.gov/eeoc/foia/letters/2013/ada_wellness_programs.html.

[14] EEOC, Amendments to Regulations Under the Americans With Disabilities Act—Proposed Rule, RIN: 3046-AB0, Fall 2014, *available at* http://www.reginfo.gov/public/do/eAgendaViewRule?pubId=201410&RIN=3046-AB02 (13 PVLR 1019, 6/9/14).

- not disclose the information to any non-agent third party, with the exception of first responders and agencies empowered to enforce the ADA.[15]

To keep the health information separate from decision-makers, employers offering voluntary wellness programs subject to the ADA often rely on a third-party service provider to administer the program. Employers should also consider delegating the administration of ''wellness wearables'' to such service providers to reduce ADA-related risks.

Unauthorized acquisition of that protected health information could trigger an obligation to provide breach notifications to affected individuals.

The ADA is not the only law relevant to the use of wearables for wellness programs. If the wellness program offers specific health benefits beyond tracking, such as diagnoses based on the information collected, the program likely would be subject to the Employee Retirement Income Security Act (ERISA).[16] In that case, ERISA could, depending on the structure of the program, impose potentially burdensome reporting and documentation requirements. Health benefit programs subject to ERISA must also comply with the requirements of the Health Insurance Portability and Accountability Act (HIPAA),[17] which would require the employer to take several steps similar to those required by the ADA as well as others. The employer, for example, would be required to enter into a business associate agreement with any service provider that collects information recorded by wearable health trackers and would otherwise need to integrate the wellness program into the organization's overall HIPAA compliance program.[18]

To the extent the wearable collects health information protected by HIPAA, the employer must safeguard the information.[19] Unauthorized acquisition of that protected health information could trigger an obligation to provide breach notifications to affected individuals.[20] In addition, several states require breach notifications when the breach implicates health information.[21]

Wellness programs are a relatively direct example of how employers might use wearable devices to collect health information from employees. Employers also might gather health information more indirectly from a wide range of wearable devices. For example, a video of an equipment malfunction taken by a technician with Google Glass might inadvertently reveal a tremor caused by Parkinson's disease. A device that used the employee's cardiac rhythm to authenticate her identity also might expose her atrial fibrillation. Consequently, before providing any type of wearable device to employees, employers should carefully assess whether the device will collect health information directly or indirectly and consider the implications with respect to the ADA, HIPAA and any other applicable law.

b) Non-Health Information

Wearables may collect not only health data, but also a wide range of other information about the employee wearing the device. For example, tracking devices might record an employee's location not only at work, but also while on break or during meal periods. Other devices could record a worker's unique patterns of movement, such as hand movements during surgery using special gloves that facilitate microscopic surgery. Although employers' collection of this type of non-health information from an employee using a wearable device is not heavily regulated in the U.S., collecting such non-health information still could present not just legal risks but also risks to employee morale.

In a unionized workplace, the collection of non-health data could be a mandatory subject of collective bargaining.

At least two states impose strict limitations on the collection of biometric identifiers. Biometric identifiers are physical markers that uniquely identify an individual, such as fingerprints or retina scans. An employer might use biometric data gathered by a wearable, for example, to authenticate access to the employer's computer system or to a highly secure area of the employer's facilities. Texas and Illinois require that an individual consent to the capture of his or her biometric identifier for a commercial purpose.[22] The biometric identifier in these states must also be protected as confidential information and destroyed within a reasonable time.[23]

Taking wearables to the next level might involve the implantation of a microchip into the employee. At least four states—including California, Oklahoma, North Dakota and Wisconsin—prohibit employers from requiring employees to implant microchips.[24]

Finally, in a unionized workplace, the collection of non-health data could be a mandatory subject of collec-

[15] *See* 42 U.S.C. § 12112(d)(4)(C).

[16] *See, e.g.*, 29 U.S.C. § 1191b(a)(2) (defining ''medical care'' broadly).

[17] *See* 45 C.F.R. pt. 160.103 (definition of ''group health plan'').

[18] *See* 45 C.F.R. pt. 164.502(e) (disclosures to business associates).

[19] 42 U.S.C. § 1320d-2(d)(2).

[20] 45 C.F.R. pts. 164.400–414.

[21] *See, e.g.*, Cal. Civ. Code § 1798.82(e); Fla. Stat. § 501.171; Tex. Bus. & Com. Code § 521.002.

[22] 740 Ill. Comp. Stat. 14/15(b); Tex. Bus. & Com. Code § 503.001(b).

[23] 740 Ill. Comp. Stat. 14/15(e); Tex. Bus. & Com. Code § 503.001(c).

[24] *See* Cal. Civ. Code § 52.7 (''[A] person shall not require, coerce, or compel any other individual to undergo the subcutaneous implanting of an identification device.''); N.D. Cent. Code § 12.1-15-06 (''A person may not require that an individual have inserted into that individual's body a microchip containing a radio frequency identification device''); Okla. Stat. tit. 63, § 1-1430 (''No person, state, county, or local governmental entity or corporate entity may require an individual to undergo the implanting of a microchip or permanent mark of any kind or nature upon the individual.''); Wis. Stat. § 146.25(1) (''No person may require an individual to undergo the implanting of a microchip.'').

   ISSN 1538-3423

tive bargaining. Failing to bargain, or violating the collective bargaining agreement by mishandling the data, could lead to an unfair labor practices charge.

While these legal risks are somewhat peripheral, the potential for damage to employee morale resulting from the use of employer-provided wearables in the workplace is very real. In its survey, PricewaterhouseCoopers found that 82 percent of respondents were concerned that wearables would invade their privacy and 86 percent thought that wearables would make them more vulnerable to data security breaches.[25] Many employees likely would balk at participating in a wearables program, regardless of its legal justification, unless they fully understood how the information collected about them by the wearable device would be used. Others might simply be daunted by the novelty of the technology. Employee resistance could undermine the efficiencies the wearables are intended to achieve and result in the employer's failure to recoup its investment in the devices.

To mitigate these employee relations concerns, employers should consider applying the following three key lessons from past efforts to introduce new technologies into the workplace:

1. Use should be fully voluntary, at least at first. Other employees will be more likely to embrace the technology after witnessing the benefits obtained by those employees who volunteer. In addition, the early adopters may shake out any bugs in the wearable program before the wearables are more broadly rolled out to the workforce.

2. Employers should provide robust notice to wearers that explains, at minimum, the following:
   - how the technology works;
   - how the technology will enhance employees' performance or make their work easier to accomplish;
   - the information that is collected, to whom it will be disclosed, how it will be used and how long it will be retained; and
   - how access to any information collected will be controlled and any other safeguards for the information.

3. To reduce the risk of inadvertently disclosing information that employees might not want revealed, information collected by the wearable device should be de-identified, if possible. In addition, the employer should consider retaining the information for the shortest possible period necessary, especially if the data could be discoverable in civil litigation.

2. Information Collected About Individuals Other Than the Wearer

Wearables that collect information about others through visual or audio sensors or recording, such as history-recording devices and performance enhancers, create risks under state wiretap laws, other state statutes and the common law. Recording audio without the consent of all those present could violate the wiretap laws of 12 states if individuals would not expect their conversations to be recorded.[26] Employers in these states should carefully consider how to obtain consent in situations where individuals other than the employee wearing the device might be unwittingly recorded. Employers potentially could obtain the implicit consent of all employees by distributing a policy that puts employees on notice of the recording. The matter becomes more complicated, however, when wearable devices inadvertently record non-employees, such as customers, vendors or business partners. To avoid these situations, the employer might consider adopting strict rules prohibiting use of the devices outside of employee-only spaces or requiring the wearer to disable any audio recording functionality when non-employees are present.

Employers potentially face liability under wiretap laws for unauthorized recordings by employees wearing the devices.

The issue becomes even more complex in California, where several courts have construed the state's all-party consent wiretap law to encompass video recordings even when the recording captured no voice. In *People v. Gibbons*, the court ruled that videotaping sexual intercourse without consent violated California's wiretap law.[27] The court reasoned that sexual intercourse is a form of communication protected by the wiretap law.[28] Some California courts have rejected the extension of the state's wiretap law to video-only recording, but several courts have followed *Gibbons*.[29]

As the providers of these devices and the parties setting policies for their use, employers potentially face liability under wiretap laws for unauthorized recordings by employees wearing the devices. Under the same laws, the wearer of the device must also consent to being recorded, but the wearer's consent may be less of an issue because, at least in circumstances where users understand the technology, users' consent potentially can be implied from their decision to wear the device.[30]

[25] Wearable Future, *supra* note 1.

[26] Cal. Penal Code § § 631–632; Conn. Gen. Stat. § 52-570D(A); Del. Code Ann. tit. 23, § 1335; Fla. Stat. § 934.03; Md. Code Ann. Cts. & Jud. Proc. § 10-402; Mass. Gen. Laws ch. 272, § 99; Mich. Comp. Laws § 750.539; Mont. Code Ann. § 45-8-213; Nev. Rev. Stat. § 200.620; N.H. Rev. Stat. Ann. § 570-A:2; 18 Pa. Cons. Stat. § § 5703–5704; Wash. Rev. Code § 9.73.030.

[27] *People v. Gibbons*, 215 Cal. App. 3d 1204 (Cal. Ct. App. 1989).

[28] *Id.*

[29] *See, e.g.*, *People v. Nakai*, 183 Cal. App. 4th 499 (Cal. Ct. App. 2010) (arguably expanding on *Gibbons* by holding that sending a photograph over the Internet to another person qualified as a communication); *People v. Nazary*, 191 Cal. App. 4th 727 (Cal. Ct. App. 2010) (citing *Gibbons* approvingly); *but see People v. Drennan*, 84 Cal. App. 4th 1349, 1355 (Cal. Ct. App. 2000) (The ''statute is replete with words indicating the Legislature's intent to protect only sound-based or symbol-based communications.'').

[30] *Hay v. Burns Cascade Co.*, No. 5:06-CV-0137 (NAM/DEP), 2009 BL 31202 at *9 (N.D.N.Y. Feb. 18, 2009) (noting that implied consent is '' 'consent in fact' which is inferred from surrounding circumstances indicating that the [party] knowingly agreed to the surveillance'' (modification in original, internal quotation omitted)).

Several states also make it unlawful to record audio or video in locations, such as restrooms and changing areas, where individuals reasonably can expect privacy.[31] An employer potentially could face liability under these laws when an employee wearing a device with video recording capability takes a bathroom break and videotapes others in this private setting, even inadvertently. Recording in these situations also potentially could trigger liability under the common law tort of intrusion upon seclusion.[32]

Not only the collection, but also the misuse of collected information, may trigger legal liability. In a not uncommon scenario, an employee tapes another employee engaging in inappropriate conduct, say sexual harassment. The employer would like to use this evidence against the harasser. Many all-party consent wiretap laws, however, prohibit using or disclosing the fruits of an unlawful recording.[33] Assuming the harassing employee was taped without his or her consent, the employer's use of the recording potentially would violate state wiretap law. In addition, embarrassing photos or video uploaded to media-sharing sites, like YouTube or Instagram, could trigger liability under the tort of unreasonable disclosure of private facts.[34]

Putting aside possible legal liability, many people could be offended by the collection of video or audio about them without their consent. Consequently, recording without notice or consent can cause employee or customer dissatisfaction and public relations problems even if no legal liability is created.

EU data protection laws impose tight restrictions on the use of video surveillance cameras and biometrics in the workplace.

Given the consent requirements and risks related to misuse, employers who introduce wearables into their workplace that are capable of capturing information about others should consider taking the following steps to mitigate risk:

1. ensure employees fully understand the device's information-gathering capabilities to avoid situations in which data are collected inadvertently;
2. use the device's own functionality, where technically feasible, to restrict the collection of information to the work-related purpose for which the wearables are being used;
3. establish policies to safeguard, and otherwise limit access to and disclosure of, the information collected by the wearables and require those with authorized access to use the information only for the purposes for which the information was collected;
4. establish policies on employees' use of the wearables to mitigate risk, such as prohibiting wearables in locations where employees have a reasonable expectation of privacy and requiring the wearer to provide notice of, or to deactivate, any audio or video recording capability when nonemployees are present; and
5. train both the users of the wearables and those with access to the information generated by the wearables on the risks and how to mitigate them.

B. Employer-Provided Wearables Outside the U.S.

Detailed coverage of the use of wearables by non-U.S. employers generally is beyond the scope of this article. However, it is worth noting that European Union data protection laws impose tight restrictions on the use of video surveillance cameras and biometrics in the workplace. In France, employers may not install surveillance cameras in the workplace without legitimate reasons, such as to investigate theft. The French data protection authority, the Commission nationale de l'informatique et des libertés (CNIL), recently issued a public notice against a seller of computer equipment for allegedly maintaining an excessive number of surveillance cameras aimed at employees in stores.[35] Wearable devices that record video could quickly run afoul of these laws and similar laws in other EU jurisdictions.

In several EU countries, biometric information is classified as sensitive personal information which entails a host of restrictions.[36] Employers must typically obtain express consent from employees in these countries before handling their biometric data, and they also must register with the local data protection authority.

U.S. multinational employers also should note that many countries outside the EU have adopted broad data protection laws, often based, in whole or in part, on the EU model. For example, biometric information also is classified as sensitive personal information in Australia, India and Colombia and subject to restrictions similar to those applicable in the EU.

Given the restrictions in these countries, U.S. multinationals likely will have much more difficulty introducing wearables into the workplace in the EU and in other jurisdictions with similar data protection regimes. These tighter legal restrictions might not make much difference as a practical matter—at least for now. The U.S. accounts for the lion's share of the wearable tech market. Analysts estimate that 40 percent of wearable technology devices are consumed in the U.S.[37] Although other regions may ultimately catch up with the U.S., for the time being, wearables have not gained much traction outside the U.S.

[31] *See, e.g.*, Ariz. Rev. Stat. § 13-3019; R.I. Gen. Laws § 28-6.12-1.

[32] *See* Restatement (Second) of Torts § 652B.

[33] *See, e.g.*, Fla. Stat. § § 934.03(d), (e); Mass. Gen. Laws ch. 272, § 99(C)(3).

[34] *See* Restatement (Second) of Torts § 652D.

[35] CNIL, Vidéosurveillance au travail: mise en demeure de la société APPLE RETAIL France, Oct. 30, 2014, *available in French at* http://www.cnil.fr/linstitution/actualite/article/article/videosurveillance-au-travail-mise-en-demeure-de-la-societe-apple-retail-france (13 PVLR 1960, 11/10/14).

[36] *See, e.g.*, Office for Personal Data Protection from the Czech Republic, Privacy protection in the workplace: Guide for Employees, at 3.6.2, *available at* http://bit.ly/1BxkZ0k.

[37] *Wearable Technology Shipments Expect to Reach $135 Million by 2018*, Business 2 Community, Aug. 26, 2014, *available at* http://www.business2community.com/tech-gadgets/wearable-technology-shipments-expect-reach-135-million-2018-0987772.

  PVLR ISSN 1538-3423

C. Employee-Owned Wearables

Employee-owned wearables introduce a separate set of legal issues for businesses. Many employers will have to grapple with these issues soon, if such issues have not surfaced already. According to a PricewaterhouseCoopers survey, one in 10 Americans wore wearable technology on a daily basis in 2014.[38] This suggests that millions of Americans already wear their devices to work. Employers also can expect the number of such employees to increase with growing adoption rates.

1. Employee-Owned Wearables That Collect Information About Others

Imagine a workplace in which employees clad in history-recording wearables walk around streaming to a public website everything seen and heard by their *personal* wearable device. This is the nightmare scenario for employers. Other employees would have legitimate claims of invasion of privacy, especially if caught in embarrassing situations. The recordings may also reveal the employer's trade secrets and other confidential information, such as confidential manufacturing processes. Recording need not be continuous to raise these risks of course. The occasional, even accidental, recording of the workplace by an employee unfamiliar with all of the capabilities of his or her wearable device could achieve the same effect. For many employers, the simple solution might appear to be banning employees from bringing their wearable devices to work altogether—or at least those with audio and/or video sensing and/or recording capability.

A ban on recording in the workplace justified by legitimate reasons could be defensible under the NLRA.

Such a total ban could be a challenge to implement. The National Labor Relations Board has interpreted the National Labor Relations Act (NLRA)[39] to prohibit some employer prohibitions on photographs and video in the workplace. The NLRA has reasoned that no-recording policies could interfere with employees' rights to protest the conditions of their employment, for example, by documenting unsafe working conditions.[40]

While the law in this area remains unsettled, a ban on recording in the workplace justified by legitimate reasons could be defensible under the NLRA. In *Whole Foods Market, Inc.*, for example, an administrative law judge upheld the employer's general prohibition on all audio recordings in the workplace without prior management approval on the grounds that the employer had imposed the ban for legitimate business reasons.[41] The evidence showed that Whole Foods had promulgated the ban to thwart the ''chilling effect'' of workplace audio recording.[42] The company's ''no recording policy'' explained the company's concern that audio recording ''can inhibit spontaneous and honest dialogue especially when sensitive or confidential matters are being discussed,'' and the evidence showed that employees routinely participated in meetings where candid discussion was expected.[43]

Like Whole Foods, employers wishing to ban from their workplace employee-owned, history-recording and other wearables that record or stream audio and/or video should consider drafting a policy that justifies the ban in a way that mitigates NLRA-related risk. The policy should provide examples of specific situations where recording in the workplace would inhibit frank discussion, threaten the employer's confidential information or violate state law because the employer did business in an all-party consent jurisdiction and employees routinely interacted with non-employees as part of their jobs. The policy should apply to all employees, not just to non-management employees, to avoid suggesting that the employer's real motive is to hinder non-management employees from engaging in activities protected by the NLRA, such as recording and reporting unsafe working conditions. The employer also should avoid promulgating the policy in response to union activity, such as a union organizing campaign. Finally, before disciplining an employee who used a wearable to record communications in the workplace without management approval, the employer should carefully analyze whether the recording itself could be considered an exercise of the employee's protected rights under the NLRA.

In the alternative, employers might consider a ban targeted only toward the activity the employer finds objectionable. For example, an administrative law judge in *Verizon Wireless* found that a prohibition only on nonconsensual recording was sufficiently tailored to protect privacy concerns without impeding employees' right to engage in concerted activity.[44] A similar approach would be to prohibit employees from wearing wearables with recording capabilities unless they notified all those present that they were being recorded, or to prohibit wearables in areas where employees or customers had an expectation of privacy, such as locker rooms, restrooms or changing areas.

2. Employee-Owned Wearables That Collect Information Only About the Wearer

Personal wearables that collect information only about the wearer, such as fitness trackers and health trackers, raise fewer concerns. Nonetheless, these wearables present some risks for employers.

Such devices could, for example, be a distraction and reduce productivity. As a general rule, employers are not required to allow employees to bring fitness or health trackers into the workplace. In a case where the device is a reasonable accommodation for a disability, however, the employer may be required to allow the employee to wear it.[45] For example, a health tracker that monitors blood sugar might be a reasonable accommodation under the ADA for an employee with dia-

[38] Wearable Future, *supra* note 1.

[39] 29 U.S.C. § § 151–169.

[40] *See, e.g.*, Prof'l Elec. Contractors of Conn., Inc., No. 34-CA-071532 (N.L.R.B. A.L.J. June 4, 2014).

[41] Whole Foods Mkt., Inc., No. 01-CA-096965 (N.L.R.B. A.L.J. Oct. 30, 2013).

[42] *Id.*

[43] *Id.*

[44] Verizon Wireless, No. 21-CA-075867 (N.L.R.B. A.L.J. July 25, 2014).

[45] *See* 42 U.S.C. § 12112(b)(5).

betes. Even where a health tracker or other wearable does constitute a reasonable accommodation, an employer still can restrict the employee's use of the device to prevent the use from interfering with the performance of essential job functions.[46] For example, a customer-service employee could be required not to check a report generated by a health tracker during a customer interaction.

Where an employer does permit employees to use personal wearables at work, managers should be instructed *not* to seek information generated by the wearable.

Where an employer does permit employees to use personal wearables at work, managers should be instructed *not* to seek information generated by the wearable. Such inquiries may create significant legal risks. For example, access to information generated by a personal health or fitness tracker could trigger liability under computer trespass laws, the tort of invasion of privacy or the ADA.

Accessing information stored on an employee's wearable device or stored in an account at a service provider accessible via the wearable could violate federal or state laws that prohibit computer trespass. The federal Computer Fraud and Abuse Act and state computer trespass laws generally prohibit accessing a computer without authorization.[47] Courts have interpreted ''computer'' very broadly to apply even to ''flip phones'' that only make calls and send and receive text messages without Internet access or application functionality.[48] Consequently, many forms of wearable technology likely would fall under computer trespass laws. Employers that accessed information stored on employees' personal wearables in this category without the employee's valid consent could face both civil and criminal liability under computer trespass laws.

The tort of invasion of privacy applies where the defendant has intentionally intruded into a place in which the plaintiff has a reasonable expectation of privacy in a manner that would be highly offensive to a reasonable person.[49] Accessing sensitive personal information in an employee's personal wearable device, without the employee's permission, could satisfy the elements of this tort. In addition, as discussed in more detail above, accessing health information stored on a wearable could violate the ADA's prohibition on employer inquiries into disabilities. Also, as noted above, relying on information about a disability obtained from a wearable to make an employment decision likely would violate the ADA. Even if the manager did not, in fact, rely on health information obtained from an employee's wearable to make an employment decision, the manager's knowledge of that information would make it more difficult to defend a claim of disability discrimination.

III. Conclusion

While the long list of privacy and data security risks discussed in this article may be daunting, employers should not necessarily shy away from wearables. As the examples illustrate, wearables offer unique benefits. The key to taking advantage of these benefits is recognizing that, just as privacy and data security risks are central to the technology, policies and training to reduce privacy and data security risk should be central to any wearables program. This conclusion applies with equal force to wearables owned by the employer and those owned by employees. Employers should take care not to address the risks in an ad hoc manner.

When possible, privacy and data security should be designed into the devices. In addition, or in the absence of, privacy by design, employers must commit themselves to understanding the technology—what information it gathers and with whom it is shared—and design policies that address the risks and provide meaningful training. Employers that address these risks head-on will put themselves in a position to benefit from wearables.

[46] *See id.*

[47] 18 U.S.C. § 1030(a)(5)(C).

[48] *United States v. Kramer*, 631 F.3d 900, 902–03 (8th Cir. 2011) (10 PVLR 303, 2/21/11).

[49] *See* Restatement (Second) of Torts § 652B.

  PVLR ISSN 1538-3423