MINTZ

Wearable Devices in the Workplace Challenge Data Security and Privacy

August 21, 2014 | Advisory | By Jonathan T. Cain

VIEWPOINT TOPICS

- Privacy & Cybersecurity
- Employment

RELATED PRACTICES

- Privacy & Cybersecurity
- Employee Benefits & ERISA

RELATED INDUSTRIES

Wearable devices, including health and activity monitors, video and audio recorders, location trackers, and other interconnected devices in the form of watches, wristbands, glasses, rings, bracelets, belts, gloves, earrings, and shoes are being heavily promoted in the next wave of consumer electronics.

It is estimated that 90 million wearable data devices ("WDD") will be shipped to customers in 2014. Many of these customers will bring them into the workplace, which will challenge employers to adapt employment and IT policies to these new visitors.

Corporate human resources and IT policies are not ready for this flood. WDDs present challenges to employers that are different than those they faced with smartphones and tablets. Smart employers will put policies in place now to manage the integration of WDDs into the workplace and adjust them as needs dictate. Less prepared employers will be deeply exposed to liability for data breaches, privacy and workplace discrimination complaints, and other disruptions as they try to catch up.

HR and IT policies covering WDDs should address at least the following concerns:

- Detection – Unlike a smartphone or a tablet, WDDs may not be readily detectable by other employees. Depending upon the functions the WDD performs, this may or may not present problems for management. A personal activity monitor that records an employee's steps may present few issues, but a WDD that can record audio and video of employee interactions with co-workers and customers invokes a host of privacy, workplace and data security, and customer relations concerns that demand management attention. Workplace policies should set out the circumstances under which various categories of devices may be used, and what notice is required to co-workers and customers when they are brought into the workplace.
- Security – Many (and eventually most) WDDs will include wireless capability, which may challenge the security of corporate data. Physical controls and data access protocols may be compromised by employees either intentionally or inadvertently. It is unlikely that WDDs will incorporate sophisticated data security features, which means that they pose a new channel of unauthorized third-party access to corporate data systems serving the workplace without the wearer's knowledge. Polices should address where and under what circumstances WDD wireless capability may be used.
- Privacy – The reasonable privacy expectations of co-workers and customers are challenged when employees are able to use WDDs to record their interactions. The wearer's expectations of privacy in the data that his WDD collects may also be inconsistent with the employer's views about its right to monitor and record data broadcast within its workspaces. Workplace policies should address the extent to which the employer retains the right to maintain surveillance of such transmission and the purposes for which they may be used.
- Productivity – Employers have struggled to establish the correct balance between an employee's use of personal email or web browsing on a smartphone during working hours with an employer's desire to accomplish the day's work. With WDDs, this problem may only become more challenging. The employer may need to consider modifying workplace policies to address the use of company resources and company time in the pursuit of personal interests using WDDs.
- Support – As more employees bring WDDs into the workplace, the demands upon IT departments to support them will increase. Employers need to consider whether and how they will integrate these new classes of devices into their IT environments. A simple answer may be to exclude them from IT support, but experience with smartphones has shown that this approach quickly weakens and eventually fails if there is any business reason employees can find to justify their use in the business setting.
- Liability – Allowing WDDs in the workplace suggests at least two avenues of exposure to employer liability: liability to other employees or customers who are subjected to surveillance or recording by WDDs in the workplace and liability to the WDD-wearing employees whose personal data is collected, processed, or disclosed by the employer. Policies should address the circumstances under which interactions with third parties may be recorded. Employers also should consider how they are going to limit their employees' expectations that data transmitted from a WDD over a company network will

remain private.

Mintz Levin's Privacy & Security Practice, working with our employment lawyers, is available to assist your company in preparing for the WDDs that are already in your workplace and the many more that are to come.

Authors

Jonathan T. Cain