What IG Professionals Should Know About the Internet of Bodies

Judy Vasek Sitton, CRM, FAI

Welcome to the Age of the Internet of Bodies

A company in Wisconsin had a "chipping party" in 2017 to implant microchips in some of its employees to make it easier for them to access the buildings and systems and to buy food in the company break room.[1] Those employees joined a growing number of workers in other countries – Belgium, the UK, and Sweden, to name a few – who use microchips for workplace security, convenience, and commuting. Microchips are just one example of the increasing variety of smart devices that are near to, attached to, or reside inside the human body. These devices are no longer relegated to science fiction and spy thrillers. They are in use today – and are creating a myriad of records.

Courtesy of metamorworks

[1] Graham, Jefferson and Laura Schulte. USAToday.com. "Wisconsin workers embedded with microchips." August 1, 2017.

What is the Internet of Bodies?

According to futurist Bernard Marr,[2] "The Internet of Bodies (IoB) is an extension of the IoT (Internet of Things) and basically connects the human body to a network through devices that are ingested, implanted, or connected to the body in some way. Once connected, data can be exchanged, and the body and device can be remotely monitored and controlled." Another common name for the IoB is *embodied computing*, where the human body is used as a technology platform.

Benefits and Risks

Each type of IoB device brings with it benefits and risks. Workplace safety, health monitoring, and convenience top the list of benefits. Some IoB devices can provide access to systems and workspaces without the need for passwords or key cards and can offer convenient purchases of goods or services. The devices can monitor, analyze, and alert to dangers in the workplace and can aid in health awareness and enhancement.

On the downside, because of their almost constant presence, the devices can facilitate an all-encompassing capture of personal information, intended and unintended, which, for example, can run afoul of workplace privacy laws. As with other connected devices, the tracked data can be hacked, breached, or otherwise exploited. The artificial intelligence (AI) factor in IoB devices will typically have innate biases that can distort data. Additionally, cyber-attacks against the human body through the devices is a real (and terrifying) threat.

For better or worse, legal precedents are being set for using information from devices as evidence in criminal investigations. Pacemakers, smart speakers, fitness trackers, internet-enabled appliances, smart phones, and data retrieved from a vehicle crash data recorder have all served as "witnesses" to crimes.

Types of Devices and What They are Gathering

Body-inserted devices ("embeddables"). In addition to embedded biometric microchips, other common implanted devices are cochlear implants for the ears, heart pacemakers, and blood-sugar monitors. Not as common is the fledgling brain-computer interface (BCI) announced by Elon Musk in July 2019 that seeks to enable humans to merge with AI, giving people superhuman intelligence or allowing a way for quadriplegics to control a computer or smart phone by thought. Also, in development are surgically implanted brain devices that may be able to upgrade

[2] Marr, Bernard. Forbes.com. "What Is the Internet of Bodies? And How Is It Changing Our World." December 6, 2019.

memory, restore memory for people with traumatic brain injuries, or treat diseases such as Alzheimer's or Parkinson's.

Body-external devices ("wearables"). Wearable technology began as any kind of electronic device designed to be worn on the user's body. It has since evolved to include devices that gather data while residing in close proximity to a user's body. These devices can take many forms. Included are Apple Watches that transmit location, movement, and health data and can be programmed to monitor sensor data and become a warning device; smart contact lenses that monitor glucose levels and may someday be advanced enough to record everything a person sees; health monitors used in wellness programs that collect temperature data, glucose levels, blood pressure, and more; and digital tattoos that contain a nearfield communications chip (NFC) to identify oneself, pay for goods, and monitor health. The tattoos can be peeled off or absorbed by the body after use.

Other devices in this category include radio frequency identification (RFID) tags and sensors that detect falls, gasses, and other dangers; work boots and construction vests that monitor for and prevent workplace injuries such as carpal tunnel syndrome or back injuries; smart-clothes and safety equipment with biosensors that monitor heart rate, body temperature, and other personal conditions; GPS sensors in vests that let companies know where employees are in the event of an emergency and that also measure nearness to dangerous equipment, user stress levels, and user drowsiness; and smart-glasses that record details of work performed and safety inspections and that – combined with augmented reality (AR) – can transmit and receive 3D graphics overlay information to help workers complete tasks.

There are devices that may not seem like wearables at first glance but would qualify because of their constant presence or proximity to their owner. Think about the omnipresent smart phone (now just called *phone*), seemingly always in hand, which captures photos, contains apps, and provides location data through GPS, among many other functions. Smart desks tell whether an employee has been sitting or standing for too long. A digital assistant like Alexa for Business can check the calendar, add meetings, and help locate the nearest meeting room. Alexa can also order supplies, track to-do lists, answer general knowledge questions, and (intentionally or unintentionally) listen in to conversations. Even autos and work vehicles are moving into the wearables category as they capture more and more data that identifies each individual driver's personal habits, location, and speed-limit adherence both while on the job and away from it.

Devices we eat ("ingestibles"). In the ingestibles category are Bluetooth electronic pills that monitor the inner workings of the human body. They can reveal food eaten and drugs (prescribed or illicit) that have been taken, and they monitor reactions to medications. Ingestibles can also track location, movement, heart rate, body

temperature, and blood chemistry. Under development is an electronic pill-shaped camera that will transmit images as it passes through a person's digestive system.

Legalities

Legal issues related to the IoB span the domains of privacy, ownership, ethics, and beyond. Meaningful consent given by the IoB device carrier is paramount. There are serious questions of whether tech companies can effectively protect data, the users, and IoB "nodes" from malicious hacking, and whether insurance companies should be able to increase premiums or even deny health coverage based on information generated by IoB data.

Records generated by IoB devices used in the work environment are subject to laws that regulate workplace privacy and employee monitoring. In this context, there is a real risk of inadvertently capturing or over-retaining IoB data that falls outside the intended or allowable scope of work activity. In the case of microchips, for instance, laws exist in some jurisdictions to prohibit employers from mandating that employees accept the use of personal identification microchip technology for any reason as a condition of employment. Case law is beginning to address data collection and data privacy issues associated with the IoB. One thing is clear: legislation will *not* be able to keep pace with technology. It has never been able to do so.

Considerations for IG Professionals

In the following list are key questions for IG professionals and other stakeholders who must manage IoB data:

- Who should have access to the devices or to the generated data?
- How can data be protected from those who shouldn't have access?
- Do health information privacy rules apply?
- What are the company's biometrics obligations?
- Will the employer be required to turn information over in criminal investigations?
- What is required by the General Data Protection Regulation (GDPR) or equivalent statutes for health and genetics or for sensitive personally identifiable information?
- How will old devices and any retained data be processed when no longer assigned to a person?

Next Steps

As IoB devices continue to proliferate, IG professionals will increasingly have to manage their implications in the workplace. There are steps to take that can make this task easier.

First, IG professionals must make more connections with co-workers, IT, and the business units to understand what type of information is being created.

Additionally, they should establish and disseminate formal policies. Clearly document the privacy policies surrounding devices that are trackable or that continuously record data. Tell employees what types of data might be obtained by the employer. Explain the ground rules of the data that is collected, how it is collected, and how long it is maintained. And detail not only the employer's obligations surrounding such data, but also the employees' obligations for assuring security, such as any protocols for dealing with a lost device.

Finally, be aware of the liability that the sheer volume of data amassed creates. The employer may inadvertently sweep up more information than it needs to know. Develop an audit plan and make corrections to it as needed. Know also that adverse legal action against an employee can get complicated if the employer has information about that employee's whereabouts outside of work hours. Employees may be able to claim discrimination or bias based on the quantity and types of data collected.

For More Information

Overview

FCC.gov. "Ingestibles, Wearables and Embeddables."

Ranger, Steve. ZDNet. "IoT in the office: Everything you need to know about the Internet of Things in the workplace." March 28, 2018.

ConsumerReports.org. "Guide to Digital Security & Privacy."

Uses of Ingestibles, Wearables, and Embeddables

HDI.Global. "Wearables can improve construction site safety."

Nicastro, Dom. CMSWire.com. "Examining the role of wearables technology in the workplace." August 27, 2018.

Ferguson, Alan. SafetyandHealthMagazine.com. "Ready-to-wear: Technology could boost workplace safety, but concerns remain." February 24, 2019.

McCloskey, Jimmy. The-Ambient.com. "CSI Alexa: The smart home has become the new crime scene witness." January 20, 2018.

Ismail, Kaya. CMSWire.com. “Virtual employee assistants changing workplace dynamics.” August 28, 2019.

Grauer, Yael. ArsTechnica.com. “A practical guide to microchip implants.” January 3, 2018.

Mullin, Sheppard. EyeonPrivacy.com. “FDA issues new draft cybersecurity guidance for medical devices.” November 29, 2018.

Recordkeeping Considerations

Simpson, Andrew G. InsuranceJournal.com. “Why Less Data May Be More for Employers Using Wearables in Workplace.” May 15, 2019.

Legalities

Lewis, Jackson. WorkplacePrivacyReport.com. “Key Considerations When Monitoring Employees Using GPS Tracking Devices.” September 8, 2014.

Matwyshyn, Andrea M. WSJ.com. “The ‘Internet of Bodies’ Is Here. Are Courts and Regulators Ready?” November 12, 2018.

Pauwels, Eleonore, and Denton, Sarah W. WilsonQuarterly.com. “Searching for privacy in the internet of bodies.” Spring 2018.

PrivacyRights.org. “Workplace privacy and employee monitoring.” Revised March 25, 2019.