AMA Journal of Ethics®
April 2019, Volume 21, Number 4: E356-362

STATE OF THE ART AND SCIENCE

What Are Best Practices for Ethical Use of Nanosensors for Worker Surveillance?

Gary E. Marchant, PhD, JD, MPP

Abstract

Many employers now offer workers wearable or implantable devices that can monitor their health, productivity, and wellness. Nanotechnology enables even more powerful and functional monitoring capacity for these devices. A history of workplace monitoring programs suggests that, despite nanosensors' potential benefits to employers and employees, they can only be successful and sustainable when a company's motivations for offering them are acceptable and transparent to workers. This article describes 5 best practices for motivating nano-enabled worker monitoring programs that are acceptable, effective, and ethical.

Workplace Nanoethics

Workplace applications of nanotechnology to date have primarily raised concerns about the exposure of workers in manufacturing and other jobs to potentially hazardous nanoparticle dusts.[1] However, as nanotechnology becomes more integrated into an ever-wider range and diversity of products, other occupational issues are starting to arise. One such issue is the use of nano-enabled electronic and microfluidic technologies to create powerful and miniature connected sensors that can be used for a variety of communication, monitoring, and surveillance functions. This paper addresses the ethical, legal, and policy implications of using nanosensors in mobile health (mHealth) products such as nano-enabled wearables, implants, and tattoos to monitor the activity, productivity, health, and wellness of employees. Workplace nanosensor applications have significant potential for win-win benefits by promoting the health, wellness, and productivity of workers, but they also raise profound ethical questions about employee privacy, security, and autonomy that must be carefully negotiated and managed. Accordingly, this paper suggests best practices for implementing nanotechnologies.

Workplace Nanotechnology and mHealth Products

New mHealth products such as wearables, implants, and tattoos that collect data on a person's activities, environment, location, performance, productivity, health, and other parameters have been enabled by nanotechnology.[2] The small size and novel properties of nanomaterials afford electrochemical sensors and biosensors that can monitor specific exposures, movements, and interactions.[3] The result has been the development

of wireless intelligent devices that are tiny, portable, low cost and battery free; capable of communicating with smart phones and other connected devices; and equipped with sensors that can detect and signal specific chemicals, physiological changes, motions, and environmental conditions.[4,5] Materials with these capabilities are sometimes referred to as "programmable nanomaterials."[6] These products can consist of wearable wristbands such as Fitbit or Apple Watch,[7] sensors built into clothing or equipment,[8] tattoo sensors applied to a person's skin that can monitor physiological and chemical parameters in real time,[9] and even some radio-frequency identification or memory chips that are placed under a person's skin and provide a permanent built-in identification and communication device.[2,10] Nano-enabled wearables and implants have the potential to help improve worker productivity, health, and wellness by monitoring for adverse exposures and early disease indicators, incentivizing exercise and other healthy behaviors, and tracking performance and productivity parameters.

Such applications can theoretically benefit both the employer and the employee. Employers are looking to such technologies to try to stem rising employee health care costs as well as to reduce employee absences and health impairments that affect job performance.[11] Employees seek information and incentives to be healthier and more productive.[12,13] Nanosensors could potentially enable employers and employees to cooperate in undertaking advanced technology-based monitoring to achieve these mutual goals, which Ajunwa et al have referred to as "participatory surveillance."[14]

However, technology-based workplace surveillance programs of the past have often been designed and administered in ways that are perceived by many workers as being too intrusive and heavy handed and as benefiting employers at the expense of employees and, for these reasons, have often been unpopular with workers.[14] In some cases, these programs are implemented in ways that intrude upon workers' privacy both inside and outside the workplace (eg, by constantly tracking their location) and restrict employee liberties, while workers' perception of being constantly monitored by technology generates unnecessary stress and pressure.[14] Unsurprisingly, many existing employer wellness programs have been found to provide modest if any benefits to either workers or employers in terms of decreased health expenditures, improved health behaviors, or increased productivity.[15]

The followings section provides some best practices to avoid the types of pitfalls typical of technology-based workplace surveillance programs and to encourage a true partnership between employers and employees, which will be critical to the success of workplace nano-enabled mHealth programs.

Best Practices for Legal and Ethical Use

In the United States, there are relatively few—and, at best—weak federal and state legal protections for workers from technological surveillance in the workplace.[14] This lack

of legal protections is exacerbated by the declining role of trade unions in most industries as a force to advocate for worker rights (including privacy rights) as well as the growing number of "at will" employment contract states in which employees can be fired for any reason, giving employers greater coercive powers over their employees, including through surveillance.[14] Yet, the history of surveillance efforts that are imposed on workers without employee approval demonstrate that such unilaterally imposed surveillance requirements often backfire by reducing employee morale, increasing worker turnover, and incentivizing workers to find ways to "beat the system."[14]

As nano-enabled mHealth devices increase the potential power and intrusiveness of worker monitoring programs, it is critical that employers implement such programs in cooperation with workers as that is the only way to realize in practice the significant benefits to employers and employees that are possible from such efforts. The following best practices, derived from an extensive literature on bioethics, employee management, technology acceptance, risk management, and practical experience with worker surveillance programs,[2,14,16-22] can best ensure that nano-enabled mHealth applications can be a win-win for both workers and their employers.

1. *Voluntary, not mandatory, participation*. A key element of successful, cooperative worker monitoring programs is that a worker chooses to voluntarily employ the surveillance technology used in the program. Any program in which worker monitoring devices are mandated or coerced is likely to cause employee resentment and undermine the acceptability and success of the program. For example, West Virginia recently tried to mandate that all state public school teachers download a monitoring app and use a Fitbit wearable that connects to the app—or face penalties. Responses to this mandatory program were so overwhelming and strong by teachers and supporters that the state quickly made participation voluntary.[23]

2. *Transparent data use*. Data collected by nanosensor wearables and implants from workers could be immense, and uses to which those data are applied are highly variable. To ensure workers' trust and cooperation in the program, employers should only use data collected from workers for disclosed purposes. This restriction also means that identified, individual data will not be provided to third parties without a worker's approval; data that is shared must be anonymized and aggregated. Moreover, employers should ensure that employees have access to their data and to the analyses done on that data; such disclosures will build workers' trust and participation in—and capacity to benefit from—the program.

3. *Validated technologies*. Employers should offer only mHealth products with demonstrated validity for measuring parameters of interest. Inaccurate

mHealth data is ineffective at best and might even be harmful if it provides erroneous incentives or leads to incorrect health or performance conclusions. There have already been complaints and lawsuits alleging that some commercially popular wearable health trackers provide inconsistent and inaccurate results.[24]

4. *Data collection limited to the workplace*. Nano-enabled wearables and implants might continue to be worn by a worker and potentially continue to collect data outside the workplace during nonworking hours. There have been instances of employees trying to disable such devices for nonwork times and even being disciplined or fired for such actions.[25] Worker data collected outside of working hours is less relevant to workplace performance and productivity and therefore should not be made available to employers, although employees should be given the option to access and use data generated by the technology for their own self-improvement and wellness.

5. *Secure storage*. Any time data is collected, it is vulnerable to being hacked and stolen via cyberattacks. Such attacks would likely undermine worker confidence in nanosensor mHealth programs and thus undermine their effectiveness. Employers can do 2 things to enhance the security of data collected in such programs. First, they should ensure that both the sensors on a worker and the data storage location have the best feasible cybersecurity protection. Second, employers should only keep data for as long as actively needed to fulfill the objectives for which it was collected; data that needs to be stored for longer periods in order to track long-term trends should be permanently deidentified to minimize potential for sensitive worker data to be hacked.

While such nonbinding principles have the weakness of being unenforceable, employers can benefit from implementing the best practices suggested here to achieve more sustainable and acceptable monitoring programs. The experience implementing such best practices can help build norms that can eventually be enacted into binding legal requirements.[26,27]

Partnering With Workers for Sustainable mHealth Solutions

Nanosensors have the potential to greatly enhance the utility of wearable and implanted wearables and implants. Monitoring programs that use such sensors could provide significant benefits to both workers and their employers, creating a win-win scenario by improving worker health, wellness, and productivity. However, to be successful and sustainable, such monitoring programs must be voluntary and acceptable to workers. Employers therefore share a common interest with their workers in ensuring that

workplace surveillance programs are conducted in a fair, transparent, and ethical manner. As a recent analysis of wellness programs by Ajunwa et al concluded,

> By committing to the well-settled ethical principles of informed consent, accountability, and fair use of personal health information data, wellness programs can safely navigate the ethical quagmires associated with the collection of sensitive personal health information from employees.... [and] employers may have a better chance at realizing the healthcare cost reductions that is their primary objective without undue disadvantages to the employee.[22]

The 5 best practices described above can help ensure that such programs will be acceptable and beneficial to their workers and therefore of value to both employers and employees.

References

1. Schulte P, Geraci C, Zumwalde R, Hoover M, Kuempel E. Occupational risk management of engineered nanoparticles. *J Occup. Environ Hyg*. 2008;5(4):239-249.
2. Vaddiraju S, Tomazos I, Burgess DJ, Jain FC, Papadimitrakopoulos F. Emerging synergy between nanotechnology and implantable biosensors: a review. *Biosens Bioelectron*. 2010;25(7):1553-1565.
3. Su H, Wang Y, Gu Y, Bowman L, Zhao J, Ding M. Potential applications and human biosafety of nanomaterials used in nanomedicine. *J Applied Toxicol*. 2018;38(1):3-24.
4. Ma Z, Chen P, Cheng W, et al. Highly sensitive, printable nanostructured conductive polymer wireless sensor for food spoilage detection. *Nano Lett*. 2018;18(7):4570-4575.
5. Darwish A, Hassanien AE. Wearable and implantable wireless sensor network solutions for healthcare monitoring. *Sensors (Basel)*. 2011;11(6):5561-5595.
6. Halappanavar S, Vogel U, Wallin H, Yauk CL. Promise and peril in nanomedicine: the challenges and needs for integrated systems biology approaches to define health risk. *Wiley Interdiscip Rev Nanomed Nanobiotechnol*. 2018;10(1):e1465.
7. Piwek L, Ellis DA, Andrews S, Joinson A. The rise of consumer health wearables: promise and barriers. *PLoS Med*. 2016;13(2):e1001953.
8. Huang GW, Xiao HM, Fu SY. Wearable electronics of silver-nanowire/poly(dimethylsiloxane) nanocomposite for smart clothing. *Sci Rep*. 2015;5:13971.
9. Bandodkar AJ, Jia W, Wang J. Tattoo-based wearable electrochemical devices: a review. *Electroanalysis*. 2015;27(3):562-572.
10. Michael K, Michael MG. The future prospects of embedded microchips in humans as unique identifiers: the risks versus the rewards. *Media Cult Soc*. 2013;35(1):78-86.
11. Lee J. Medical devices are going mobile, but makers face barriers. *Bloomberg Law*. July 20, 2018. https://news.bloomberglaw.com/pharma-and-life-

sciences/medical-devices-are-going-mobile-but-makers-face-barriers. Accessed October 31, 2018.
12. Nicastro D. Examining the role of wearables technology in the workplace. *CMS Wire*. August 27, 2018. https://www.cmswire.com/digital-workplace/examining-the-role-of-wearables-technology-in-the-workplace/. Accessed January 11, 2019.
13. Metz R. This company embeds microchips in its employees, and they love it. *MIT Technology Review*. August 17, 2018, https://www.technologyreview.com/s/611884/this-company-embeds-microchips-in-its-employees-and-they-love-it/. Accessed January 11, 2019.
14. Ajunwa I, Crawford K, Schultz J. Limitless worker surveillance. *Calif Law Rev*. 2017;105(3):735-776.
15. Jones D, Molitor D, Reif J. What do workplace wellness programs do? Evidence from the Illinois Workplace Wellness Study. Cambridge, MA: National Bureau of Economic Research; 2018. NBER working paper 24229. https://www.nber.org/papers/w24229.pdf. Published January 2018. Updated June 2018. Accessed October 31, 2018.
16. Schatsky D, Kumar N. Workforce superpowers: wearables are augmenting employees' abilities. *Deloitte Insights*. July 25, 2018. https://www2.deloitte.com/insights/us/en/focus/signals-for-strategists/wearable-devices-in-the-workplace.html. Accessed January 11, 2019.
17. Baicker K, Cutler D, Song Z. Workplace wellness programs can generate savings. *Health Aff (Millwood)*. 2010;29(2):304-311.
18. Fisher E, Boenink M, van der Burg S, Woodbury N. Responsible healthcare innovation: anticipatory governance of nanodiagnostics for theranostics medicine. *Expert Rev Mol Diagn*. 2012;12(8):857-870.
19. Amarasingham R, Audet AM, Bates DW, et al. Consensus statement on electronic health predictive analytics: a guiding framework to address challenges. *EGEMS (Wash DC)*. 2016;4(1):1163.
20. Federal Trade Commission. Mobile health app developers: FTC best practices. https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-app-developers-ftc-best-practices. Published April 2016. Accessed January 11, 2019.
21. UNI Global Union. Top 10 principles for workers' data privacy and protection. http://www.thefutureworldofwork.org/media/35421/uni_workers_data_protection.pdf. Published January 2018. Accessed Jan. 11, 2019.
22. Ajunwa I, Crawford K, Ford JS. Health and big data: an ethical framework for health information collection by corporate wellness programs. *J Law Med Ethics*. 2016;44(3):474-480.
23. O'Carroll E. Can your boss make you wear a Fitbit? *Christian Science Monitor*. March 15, 2018. https://www.csmonitor.com/Technology/2018/0315/Can-your-boss-make-you-wear-a-Fitbit. Accessed October 31, 2018.

24. Fung B. Is your Fitbit wrong? One woman argued hers was—and almost ended up in a legal no-man's land. *Washington Post*. August 2, 2018. https://www.washingtonpost.com/technology/2018/08/02/is-your-fitbit-wrong-one-woman-argued-it-was-almost-ended-up-legal-no-mans-land/?utm_term=.380cfa6badee. Accessed October 31, 2018.
25. Kravets D. Worker fired for disabling GPS app that tracked her 24 hours a day. *Ars Technica*. May 11, 2015. https://arstechnica.com/tech-policy/2015/05/worker-fired-for-disabling-gps-app-that-tracked-her-24-hours-a-day/. Accessed October 31, 2018.
26. Kellogg S. Every breath you take: data privacy and your wearable fitness device. *J Mo Bar*. 2015;72(2):22-29.
27. Marchant GE, Sylvester DJ, Abbott KW. Risk management principles for nanotechnology. *Nanoethics*. 2008;2(1):43-60.

Gary E. Marchant, PhD, JD, MPP is a regents' professor and the Lincoln Professor of Emerging Technologies, Law and Ethics at Arizona State University in Phoenix, where he is also the faculty director of the Center for Law, Science and Innovation at the Sandra Day O'Connor College of Law. He is also a professor at the School of Life Sciences and a distinguished sustainability scientist at the Julie Ann Wrigley Global Institute of Sustainability at Arizona State University in Tempe. His research interests include the governance of emerging technologies, legal aspects of personalized medicine, use of genetic information in the legal system, legal aspects of risk assessment and risk management, and the application of science and technology in the legal system.

Citation
AMA J Ethics. 2019;21(4):E356-362.

DOI
10.1001/amajethics.2019.356.

Conflict of Interest Disclosure
The author(s) had no conflicts of interest to disclose.

The viewpoints expressed in this article are those of the author(s) and do not necessarily reflect the views and policies of the AMA.

ISSN 2376-6980