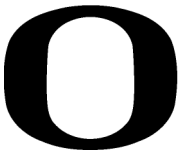
Presented to the Interdisciplinary Studies Program:



UNIVERSITY OF OREGON
APPLIED INFORMATION MANAGEMENT

Applied Information Management
and the Graduate School of the
University of Oregon
in partial fulfillment of the
requirement for the degree of
Master of Science

Augmenting Workplace Wellness Programs with Biometric Monitoring

CAPSTONE REPORT

Jason Miller
Technical Program Manager
Intel Corporation

University of Oregon
Applied Information
Management
Program

Fall 2018

Continuing and Professional
Education
1277 University of Oregon
Eugene, OR 97403-1277
(800) 824-2714

Approved by

_____

Dr. Kara McFall
Director, AIM Program

Augmenting Workplace Wellness Programs with Biometric Monitoring

Jason Miller

Intel Corporation

Abstract

This annotated bibliography contains recent research describing the practices, policies, risks, and results regarding employer-sponsored wellness programs in the United States that are increasingly augmented with biometric monitoring features such as fitness trackers. The goal of this study is to improve the understanding of common risks and shortcomings so that individuals designing or augmenting wellness programs have improved chances of achieving success in helping employees reach positive health outcomes.

Keywords: wellness program, biometric monitor, fitness tracking, dataveillance, health insurance, big data, data-proxy

Table of Contents

List of Tables and Figures

Introduction to the Annotated Bibliography

Problem

In the United States, employer-sponsored health insurance covers over half of the non-elderly population (Claxton, Rae, Long, Damico, & Whitmore, 2018); in this context, nonelderly individuals are those under the age of 65 (Henry J. Kaiser Family Foundation, 2017). Health insurance became a common benefit for employers to provide during World War II as an alternative to higher wages (Klein, 2003), but ongoing increases in healthcare costs have resulted in increasing costs for both employers and employees (Claxton et al., 2018). Claxton et al. (2018) found that for 2018, “Annual premiums for employer-sponsored family health coverage reached $19,616 this year, up 5% from last year, with workers on average paying $5,547 toward the cost of their coverage” (p. 7).

Increasing healthcare costs have prompted employers to develop cost-containment tactics (Hull & Pasquale, 2017). While two-thirds of U.S. employers assert that "employees’ poor health habits" is an obstacle to affordable health coverage (Mattke et al., 2013, p. 1), the Patient Protection and Affordable Care Act (2010) allows a group health plan to offer discounts of up to 30 percent for participation in wellness programs (Claxton et al., 2018). Employers believe that wellness programs can counteract rising health care costs and boost employee productivity (Mattke et al., 2013). As a result, 82 percent of employers with 200 or more employees now offer wellness programs to their employees (Claxton et al., 2018).

Wellness programs are generally composed of a variety of screening activities, lifestyle management activities that commonly include quitting smoking and losing weight, and behavioral health coaching (Claxton et al., 2018; Mattke et al., 2013). In recent years, these programs have added a technological component: in 2018, 21 percent of large employers used

biometric monitoring to collect information about their employees, up from 14 percent in 2017 (Claxton et al., 2018). Many employers collect biometric data from their employees in a variety of ways within the workplace, from fingerprint-reading timeclocks to *exoskeletons* that monitor worker posture (Ajunwa, 2018; Pearlman, Young, & Weinstein, 2017). However, the wellness programs are extending biometric monitoring of employees outside of the workplace using consumer-oriented wearable devices like the Fitbit *fitness tracker* to motivate people to get healthier, promising to decrease healthcare spending and allow for finely-tuned insurance premiums (Christophersen, Mørck, Langhoff, & Bjørn, 2015). Biometric data collected or inferred by these devices "will always be shared with the device maker and a range of unknown others" (Crawford, Lingel, & Karppi, 2015, p. 486), differentiating this internet-connected method of self-measurement and awareness from earlier physical-bound techniques dating back to antiquity that Foucault (1985) described in detail. For example, the humble bathroom scale only reports its user's weight to the user while the user is standing upon it, but internet-connected biometric tracking devices will record and share data collected from their users with their manufacturers for aggregation and analysis (Crawford et al., 2015).

Many consumers are only vaguely aware of what happens to the data collected from them by their wearable devices (Becker, 2018). Their ignorance is partially a side-effect of the asymmetric relationship between the individual device user generating the data and the groups who are collecting, mining, and aggregating the data from all of their individual device users (Andrejevic, 2014). The mass of individuals' data is analyzed as Big Data (Andrejevic, 2014; Latonero, 2018; Ruckenstein & Schüll, 2017). Big Data is not just an exceptionally large set of data, but rather can be thought of as

a cultural, technological, and scholarly phenomenon that rests on the interplay of:

> (1) Technology: maximizing computation power and algorithmic accuracy to gather, analyze, link, and compare large data sets.
>
> (2) Analysis: drawing on large data sets to identify patterns in order to make economic, social, technical, and legal claims.
>
> (3) Mythology: the widespread belief that large data sets offer a higher form of intelligence and knowledge that can generate insights that were previously impossible, with the aura of truth, objectivity, and accuracy. (boyd & Crawford, 2012, p. 663)

This massive amount of biometric data is of interest to insurers and employers who want to identify habits that correlate to risks for expensive health conditions (Hull & Pasquale, 2017), such as a sedentary lifestyle correlating to heart disease (Lakka et al., 2002). Chun (2016) explains that

> On at least three levels, data analytics are about habits: one, they focus on habitual actions, such as buying lotions and vitamins; two, based on this analysis, they seek to change habits, especially by focusing on moments of 'crisis'—moments of state change—such as pregnancy; and three, they 'replace' causality with correlations between habits. That is, correlations between correlations rather than correlations between repeated series of events are key. (p. 57)

Cataloging risk factors for disease is just one use of the biometric Big Data; many wearable device manufacturers also resell their collected data to secondary customers, often, but not exclusively, for marketing purposes (Crawford et al., 2015; Till, 2014). While some consumers are more bothered by this practice than others (Becker, 2018; Till, 2014), the tension "between a person's desire for self-knowledge and the way in which that person is known by a range of third parties, some with interests that may directly conflict with their own" (Crawford et

al., 2015, p. 481) is a common feature of consumer biometric tracking systems. The inclusion of biometric tracking in wellness programs makes the relationship far more complex: the wearable device manufacturer can market data analysis to the health insurance issuer that will offer discounts to employers if their employees use the wearable devices, regardless of the employees' degree of desire for self-knowledge, and thus the employees provide biometric data to the wearable device manufacturer, which can be subsequently re-packaged and resold (Crawford et al., 2015; Till, 2014).

Despite the growing popularity of this system, it presents three clear risks to employers (Ajunwa, 2018; Becker, 2018; Christophersen, Mørck, Langhoff, & Bjørn, 2015; Hull & Pasquale, 2017; Lamkin, 2013; Madden, 2017; Pearlman, Young, & Weinstein, 2017; Smith, 2016; Terry, 2012). First, the financial incentives for participating in biometric tracking could have excess influence on employees with constrained budgets (Christophersen et al., 2015). At the same time, people in a socioeconomically precarious situation are likely to expect data they provide in an asymmetric power relationship to be used against them (Eubanks, 2018; Madden, 2017; Pitcan, Marwick, & boyd, 2018). These two elements combine to create a "dilemma of forced acceptance" (Becker, 2018, p. 3266) where employees expect to be functionally betrayed but also do not believe they have alternatives, negating their capacities for providing informed consent (Lamkin, 2013).

Second, the regulatory landscape is changing and introducing and foreshadowing new regulatory compliance risks to existing practices (Pearlman et al., 2017). Within the United States, gaps in federal privacy regulations have been very permissive of both employee surveillance and the sale or exchange of data (Terry, 2012). Lacking federal leadership, states are implementing piecemeal legal protections for biometric data (Pearlman et al., 2017). Illinois,

which saw at least 26 employment class action suits regarding biometric data filed from July to October 2017, as well as Texas and Washington, have already passed legislation to protect biometric data, and five other states were considering similar legislation in 2017 (Pearlman et al., 2017). Additionally, the United States District Court for the Northern District of California has ruled that employer imposition of excessive *dataveillance* on employees outside of the workplace practically extends the workplace and thus the employer's legal responsibilities to its employees (O'Connor v. Uber Technologies, Inc., 2015). Lupton (2016), Terry (2012) and Till (2014) all acknowledge that digital *biocapital* expropriated from employees via biometric monitoring is valuable; the inherent value of the data exacerbates the risk of extended employer responsibility that the O'Connor v. Uber Technologies, Inc. (2015) ruling raises because the conscious generation of valuable material at the behest of an employer is employee labor (Smith, 2016).

International policy may also warrant attention; the General Data Protection Regulation (GDPR) requires that all organizations that collect or process EU citizens' personal data – information by which a person may be directly or indirectly identified – adhere to particular data handling and security standards and grant EU citizens a variety of access and control rights over their personal data, or face severe fines (Tankard, 2016; Wachter, 2018). Employers hiring European immigrants or guest workers therefore need to consider the GDPR regulations when designing their wellness plans and selecting biometric monitoring service providers (Fietkiewicz & Henkel, 2018; Wachter, 2018).

Finally, the third risk is the fiduciary risk that wellness programs and biometric tracking are a waste of company resources that do not lead to significantly positive health outcomes (Christophersen et al., 2015; Hull & Pasquale, 2017). Between the known inaccuracies of

wearable devices and their vulnerability to direct manipulation (Becker, 2018), relying on them for material support in policy decisions such as insurance discount rates is often inadvisable, regardless of how common the practice is becoming (Ajunwa, 2018).

By fully considering the risks posed by the biometric monitoring of employees outside of the workplace using consumer-oriented wearable devices, employers may be able to mitigate or even avoid these risks.

Purpose

The purpose of this annotated bibliography is to present literature that describes the risks and limitations of augmenting a corporate wellness program with ongoing biometric tracking. The research explores three key elements in creating or augmenting a wellness plan with biometric tracking: (a) current industry practices and trends, (b) how people relate to their data and how their data is understood as a proxy for them, and (c) challenges and shortcomings in converting complex wellness programs into positive health outcomes. The goal of this research is to approach the rapidly-growing trend of adding biometric tracking to wellness programs carefully, with particular attention to risk mitigation and avoidance.

Research Questions

Main question. How can an employer leverage biometric monitoring capabilities to promote good health habits among employees while mitigating the perceived threats of employee exploitation and loss of privacy?

Secondary question. What are the documented benefits of wellness programs? Are participating employees the primary beneficiaries of wellness program benefits, or are the benefits distributed unevenly?

Audience

The primary audience members for this research are Human Resources professionals who design, evaluate, adopt, or augment workplace wellness programs with active biometric tracking. These stakeholders will have clearer expectations of the outcomes they can expect from the program they are implementing and be more sensitive to the legal and ethical boundaries of such a program. This research is also likely relevant to the health insurance issuers that are designing stock wellness programs to augment coverage products, as well as third-party wellness program providers, who have an inherent interest in understanding the effectiveness of wellness programs in promoting good employee health habits and as an approach to lowering healthcare costs. Finally, biometric-tracking wearable device manufacturers considering partnership with insurance issuers or large corporations may use this research to inform their privacy policies and refine their value propositions.

Search Report

Search strategy. This line of research grew from my engagement with a social network of researchers and academics on a variety of topics; I found an overlap of interests in biometric tracking and wellness programs and developed the research from that starting point. Jo Ann Oravec's (2018) bibliography, delivered in-person at a conference I attended, included references to Kate Crawford and Frank Pasquale's research, both of whom are active on Twitter. Kate Crawford recommended looking up Deborah Lupton and Natasha Schüll, who are specialists in this research area. Ifeoma Ajunwa, who had previously collaborated with Kate Crawford on a related paper, added to Kate's recommendations by highlighting her current work.

The books and papers that were recommended and their references were generally hosted by the respective author, the publisher, or on the Social Science Research Network (SSRN).

When direct links were not available, I searched by the paper's title and author in Google Scholar to track down a copy of the paper. Jo Ann Oravec and Natasha Schüll were both kind enough to email me copies of their papers.

After I evaluated a document, I searched for the most interesting and applicable references from the document and repeated the process.

Search engines and databases. I searched for sources in Google Scholar and SSRN. Within the University of Oregon Libraries, I searched for sources in EbscoHost and HeinOnline.

Reference evaluation criteria. I also vetted material for authority, timeliness, quality, relevancy, and (lack of) bias. These criteria were put forward by the Center for Public Issues Education (n.d.).

The criteria for authority required at least two of the following: having a doctorate, being published by a respected institution, or having work cited by others who met the first two qualifications. For example, Kate Crawford and Frank Pasquale are both cited by and routinely cite other researchers, creating a halo of authority over the whole collective body of knowledge.

On the matter of timeliness, the changes that the ACA brought to employer-sponsored insurance and wellness programs in 2010 undermines the relevance of research performed on wellness programs prior to its implementation; therefore, I excluded earlier studies, despite the frequency with which they have been historically cited. Generally, I preferred sources from 2016 or later for the most topical analysis, even up to the point of research that is still forthcoming.

While some researchers did a better job of staying on the topic they proposed to cover than others, all of the work selected and reviewed is of adequate quality, with accurate grammar, spelling, and punctuation, and honors the respective publishers.

Reducing the profusion of material to topically-relevant sources required a focus on exclusions:

- I excluded material that focused on biometric tracking or the Quantified Self (QS) movement without wellness programs except where it delved into how the wearable device was handling the biometric data it collected. QS is comprised of individual consumers who proactively engage in collecting data about themselves via self-tracking technologies and are likely to socially engage with other users of those same technologies (Crawford, Lingel, & Karppi, 2015), differing from employees who may expect incentives to adopt biometric trackers and are expected to engage with each other as co-workers.
- I excluded material that focused on wellness programs without wearable devices except where it delved into incentives and shifting power relations between employer and employee or insurer and insured.
- I excluded material that focused on workplace surveillance without going into the implications of off-hours biometric tracking except where it considered the privacy risks in data handling and retention.

Not all of the material reviewed fits in this particular research niche, but each of the selected papers includes material that fits.

Regarding bias: The authors of all of the material presented support their points with citations and consider alternate points of view. No persuasive arguments are presented absent contrary claims. While certain authors use strongly opinionated language, they back up their opinions with data. Indeed, given this paper's focus on highlighting risks in order to facilitate

their mitigation, the issues that evoke strong opinions are of particular relevance to the current purpose.

Keywords. For the sake of completeness, I searched for one or more of the following keyword combinations, borrowed from the original supply of research:

- Employer-Sponsored Insurance and Wellness,
- Wearable Health-Tracking devices and Employers, and
- Wellness Programs and Privacy.

Documentation approach. I retained copies of all papers as articles in Evernote. Evernote supports both folders and tagging; I filed this project in its own specific folder and used tags to mark the strong domains of an article, such as *legal*, *technical*, or *anthropological*. Evernote articles include an optional metadata link to their sources; I ensured that all of the articles I collected included links featuring all information necessary to cite them appropriately. I annotated some notes with a specific important point from the article, or a page number or set of keywords so I could use Evernote's *find* capability to jump to the article's most insightful parts.

Annotated Bibliography

This report presents the annotated bibliography of 15 studies and articles. As a collection, the articles are intended to cover the basic trends and practices of employer-sponsored wellness programs, a history of biometric self-tracking coupled with modern dataveillance to establish a framework for the augmentation of employer-sponsored wellness programs with biometric monitoring, and potential risks and difficulties that have been encountered in doing so. The studies and articles have been divided into three sections. The first section, Current Industry Practices and Trends in Wellness Programs and Employee Biometric Monitoring, focuses on studies of wellness programs in the status quo; how they are deployed, what their effects are, and standing points of policy that shape the boundaries of these programs. The second section, How People Relate to Their Data and How Their Data is Understood as a Proxy for Them, delves into theory and frameworks. Sources in this section are particularly attentive to interpreting meanings in relationships such as the relationship between the individual and the biometric data that is collected from the individual, between that data and the individual's physical health, between the employer and the employee, and between the insurer and the client.

The final section, Challenges and Shortcomings in Converting Complex Wellness Programs Into Positive Health Outcomes, reviews articles describing ways in which wellness programs have failed to deliver on positive health outcomes for employees, have been repurposed away from their well-intended health goals, or could be abused in ways that create exploitative risks for employees or legal risks for employers. The articles have been categorized according to how their focus relates to the research questions and purpose of this report rather than their particular conclusions. The included abstracts are copied from the respective work, specifically using the official abstracts where available. The ideas presented in the summaries are

distilled from the article with the intent to faithfully represent the respective authors' findings and ideas.

Current Industry Practices and Trends in Wellness Programs and Employee Biometric Monitoring

Ajunwa, I. (2019). Algorithms at work: Productivity monitoring platforms and wearable technology as the new data-centric research agenda for employment and labor law. *St. Louis University. Law Journal 63 (forthcoming)*. Retrieved from https://ssrn.com/abstract=3247286

Abstract. Recent work technology advancements such as productivity monitoring platforms and wearable technology have given rise to new organizational behavior regarding the management of employees and also prompt new legal questions regarding the protection of workers' privacy rights. In this Essay, I argue that the proliferation of productivity monitoring applications and wearable technologies will lead to new legal controversies for employment and labor law. In Part I, I assert that productivity monitoring applications will prompt a new reckoning of the balance between the employer's pecuniary interests in monitoring productivity and the employees' privacy interests. Ironically, such applications may also be both shield and sword in regards to preventing or creating hostile work environments. In Part II of this Essay, I note the legal issues raised by the adoption of wearable technology in the workplace, notably: privacy concerns; the potential for wearable tech to be used for unlawful employment discrimination; and worker safety and workers' compensation issues. Finally, in Part III, I chart a research agenda for privacy law scholars, particularly in defining "a reasonable

expectation of privacy" for employees and in deciding legal questions over employee data collection and use.

Summary. Ajunwa asserts that employee monitoring technologies are little more than a current iteration in a long-running trend of optimizing employee time for productivity, but that they do introduce challenges and concerns around principles of data "collection limitation, purpose specification, use limitation, accountability, security notice, choice, and data minimization" (p. 31). She questions the ability of law and public policy to keep up with questions of data ownership, interpretation, and validity using a variety of court cases, as well as the framing question of whether the data should even be collected. She also engages the possibility that employee dataveillance "may also be both sword and shield in regards to preventing or creating hostile work environments" (p. 3) because such technology can be used both "for unlawful employment discrimination, and worker safety and workers' compensation issues" (p. 4). Ajunwa's work is far broader than wellness programs and covers many implementations of employee surveillance, but also specifically refers to biometric tracking in employer-sponsored wellness programs. She focuses heavily on both federal and state public policy and case law within the United States to look at how policy is being altered by current technological advancements in employee monitoring capabilities. While Ajunwa brings up the common points of employer overreach into off-hours time, the heavily incentivized push for adoption, and the common resale of employee biometric data by device vendors, her work is particularly relevant to this study because she notes risks to employers in data usage: employers may be tempted to use biometric monitoring to illegally discriminate against employees, or may have biometric monitoring data used against them by employees

demonstrating their diminished labor capacity in compensation claims. Ajunwa's documentation of legal risks to employers combined with her enumeration of data handling principles create a platform for comparing biometric monitoring capabilities that vendors provide within the context of a wellness program's anticipated benefits.

Claxton, G., Rae, M., Long, M., Damico, A., & Whitmore, H. (2018). Kaiser Family Foundation employer health benefits 2018 annual survey. *Henry J. Kaiser Family Foundation*. Retrieved from http://files.kff.org/attachment/Report-Employer-Health-Benefits-Annual-Survey-2018

Abstract. This annual survey of employers provides a detailed look at trends in employer-sponsored health coverage, including premiums, employee contributions, cost-sharing provisions, offer rates, wellness programs, and employer practices. The 2018 survey included 2,160 interviews with non-federal public and private firms. Annual premiums for employer-sponsored family health coverage reached $19,616 this year, up 5% from last year, with workers on average paying $5,547 toward the cost of their coverage. The average deductible among covered workers in a plan with a general annual deductible is $1,573 for single coverage. Fifty-six percent of small firms and 98% of large firms offer health benefits to at least some of their workers, with an overall offer rate of 57%. Survey results are released in several formats, including a full report with downloadable tables on a variety of topics, a summary of findings, and an article published in the journal Health Affairs.

Summary. The Kaiser Family foundation collected data from HR managers through "a telephone survey of 2,160 randomly selected non-federal public and private employers with three or more workers" (p. 18), with a 32 percent response rate. "The Kaiser Family

Foundation (KFF) has conducted this annual survey of employer-sponsored health benefits since 1999" (p. 21). The researchers found that health insurance premium costs were increasing faster than wages and inflation, and that this is a trend that has been continuous since the turn of the century. Additionally, "Deductibles have increased in recent years due to higher deductibles within plan types and higher enrollment in HDHP/SOs [High-Deductible Health Plans with a Savings Option]" (p. 13), but "The growth in HDHP/SO enrollment has stalled over the past three years, which may be a sign of employer reluctance to rock the benefit boat for their workers" (p. 18). They find that 81 percent of large firms – those with at least 200 workers – have some sort of wellness program, including "health risk assessments, biometric screenings, and health promotion programs" (p. 15), with incentives for participation growing in sophistication as the programs become more complex. Biometric monitoring is an increasingly common element of these programs: "21% of large firms collect information from workers' mobile apps or wearable devices, such as a Fitbit or Apple Watch, as part of their wellness or health promotion program" (p. 198), increased from 14 percent in 2017.

This article is important to the study because it establishes the prevalence of wellness programs among large firms, as well as the growth of biometric tracking as part of those wellness programs. This is the basis for the engaging in a literature review on this subject matter for the audience specified, starting with the types of HR managers who may have been surveyed for the KFF report. This article allows the reader to orient their current position within the larger community of practice. Finally, the attention the authors paid to the ways that employees are excluded from employer-sponsored insurance is important to mapping edge cases in wellness program participation.

Fronstin, P. & Roebuck, M.C. (2015). Financial incentives, workplace wellness program participation, and utilization of health care services and spending. *Employee Benefit Research Institute Issue Brief 417*, 1-23. Retrieved from https://ssrn.com/abstract=2652794

Abstract. This paper analyzes data from a large employer that enhanced financial incentives to encourage participation in its workplace wellness programs. It examines, first, the effect of financial incentives on wellness program participation, and second, it estimates the impact of wellness program participation on utilization of health care services and spending. The Patient Protection and Affordable Care Act of 2010 (PPACA) allows employers to provide financial incentives of as much as 30 percent of the total cost of coverage when tied to participation in a wellness program. Participation in health risk assessments (HRAs) increased by 50 percentage points among members of unions that bargained in the incentive, and increased 22 percentage points among non-union employees. Participation in the biometric screening program increased 55 percentage points when financial incentives were provided. Biometric screenings led to an average increase of 0.31 annual prescription drug fills, with related spending higher by $56 per member per year. Otherwise, no significant effects of participation in HRAs or biometric screenings on utilization of health care services and spending were found. The largest increase in medication utilization as a result of biometric screening was for statins, which are widely used to treat high cholesterol. This therapeutic class accounted for one-sixth of the overall increase in prescription drug utilization. Second were antidepressants, followed by ACE inhibitors (for hypertension), and thyroid hormones (for hypothyroidism). Biometric screening also led to significantly higher utilization of

biologic response modifiers and immunosuppressants. These specialty medications are used to treat autoimmune diseases, such as rheumatoid arthritis and multiple sclerosis, and are relatively expensive compared with non-specialty medications. The added spending associated with the combined increase in fills of 0.02 was $27 per member per year -- about one-half of the overall increase in prescription drug spending from those who participated in biometric screenings.

Summary. The authors found that providing incentives "on the order of $240 per employee per year" (p. 19) increases participation in health risk assessments and biometric screening; they found that incentives increased non-union members' participation in biometric screening by 55 percent. The only substantial change in health care utilization resulting from the wellness program was biometric screening leading "to an average increase of 0.31 annual prescription drug fills, with related spending higher by $56 per member per year" (p. 1). Common prescriptions that were initiated after the biometric screening included statins, antidepressants, ACE inhibitors, thyroid hormones, biologic response modifiers, and immunosuppressants to treat autoimmune diseases. These drugs are all focused on managing or mitigating chronic disease and related risks through pharmacotherapy. The highest average baseline annual health care spending was $3,679 for non-union members.

The research tested the use of incentives to increase enrollment in a wellness program at a large employer. The study included 71,982 employees from across the United States, both union and non-union, between 2011 and 2013. The research does not extend into ongoing biometric monitoring. It also explicitly excludes reporting on "Spouses, partners, and other dependents" (p. 10). It grants that the study participants had "relatively high

earnings" (p. 14); the correlation of incentives to participation is not tested for very high or low income employees. The study also stopped short of making evaluations of "reductions in utilization of health care services and spending" (p. 19) past the first year of the study.

This research is relevant to this study because it allows an employer to calibrate their expected investment in a wellness program that achieves measurable changes in employee health habits. This baseline can then be used to evaluate the outcomes of subsequent alterations to wellness programs, including adding biometric monitoring.

Mattke, S., Liu, H., Caloyeras, J., Huang, C., Van Busum, K., Khodyadov, D., & Shier, V. (2013). *Workplace wellness programs study: Final report.* Santa Monica, CA: RAND Corporation. Retrieved from https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR254/RAND_RR254.pdf

Abstract. Out of concern about the impact of chronic disease on employee health and well-being, the cost of health care coverage, and competitiveness, employers are adopting health promotion and disease prevention strategies, commonly referred to as workplace wellness programs. Disease prevention programs aim either to prevent the onset of diseases (primary prevention) or to diagnose and treat disease at an early stage before complications occur (secondary prevention). Primary prevention addresses health-related behaviors and risk factors—for example, by encouraging a diet with lower fat and caloric content to prevent the onset of diabetes mellitus. Secondary prevention attempts to improve disease control—for example, by promoting medication adherence for patients with asthma to avoid symptom exacerbations that can lead to hospitalization. Health

promotion is related to disease prevention in that it aims at fostering better health through behavior change. A broad range of benefits are offered under the label “workplace wellness,” from multi-component programs to single interventions, and benefits can be offered by employers directly, through a vendor, group health plans, or a combination of both.

Summary. This research report, sponsored by the U.S. Department of Labor and U.S. Department of Health and Human Services, establishes a baseline of efficacy for workplace wellness programs after the policy changes contained in the ACA. It concludes that the research supports "positive effects of worksite wellness programs on health-related behavior and health risks among program participants" (p. xviii). Regarding employee participation, it found that while 69 percent of employers offered financial incentives for participation at the time of publication, only 46 percent of employees participated in screening or engaged in a risk assessment, and less than 20 percent of the employees identified for intervention activities chose to participate in them.

The report identifies a wide range of incentive values, management structures, and qualification triggers. While employers were consistently confident in the benefits of their workplace wellness programs, only 44 percent regularly evaluated their wellness programs "and only 2 percent provided actual savings estimates" (p. 53). The report describes running a simulation based on Care Continuum Alliance data from 2005 to 2010 comparing health care costs for workplace wellness program participants to those of other employees, "implying average annual cost reductions of $157" (p. 55) due to divergence in health care costs between participants and non-participants, but warning

that their "estimates are not statistically significant at the 5 percent confidence level" (p. 57). The researchers also did not have access to the costs of workplace wellness programs to determine the net value of workplace wellness program participation.

In terms of efficacy, weight loss programs averaged just under 1 pound per person per year across three years. While the typical wellness program incentives for smoking cessation were more than 3 times the participation incentive, they were still expected to be inadequate for ensuring "long-term behavior change" (p. xxiii). The researchers concluded that the benefits of behavior changes resulting from incentives were "small and unlikely to be clinically meaningful" (p. xxiii).

The report asserts that successful wellness programs feature effective communication strategies, opportunities for employees to engage, comprehensive leadership engagement, leveraging of existing relationships and resources, and continuous evaluation, noting however that "in spite of their popularity among employers, the impact of wellness programs are rarely formally evaluated" (p. xxv). The report indicates that its survey-based data is vulnerable to response bias and many of the conclusions the researchers drew were interpolated from a wide variety of wellness program designs across diverse demographics. Additionally, this report does not consider the effects of biometric monitoring technology on wellness programs, as that practice was not common at the time of publication (2013).

This research is valuable to this literature review because it establishes how little is commonly expected of employer-sponsored wellness programs in short-term positive health outcomes or cost savings and makes clear that wellness programs should be designed with success metrics that are both clear and realistic.

Terry, N. (2012). Protecting patient privacy in the age of Big Data. *UMKC Law Review 81*(2). 385-415. Retrieved from https://heinonline.org/HOL/P?h=hein.journals/umkc81&i=397

Abstract. This article takes the position that, beyond its generalized threat to privacy, big data poses an exceptional group of problems for health care, its providers, researchers, and patients. Rightly or wrongly, policymakers have agreed that patient information is deserving of elevated protection compared to other data (so-called health privacy exceptionalism). Yet, at the same time, the last two administrations, one Republican and one Democrat, have promoted the dramatic growth of electronic medical records ("EMR")' with the specific goal of increasing the collection of clinical data and its broad sharing. As recently noted by the Institute of Medicine ("loM"), "the U.S. health care system now is characterized by more to do, more to know, and more to manage than at any time in history."* Technology, not surprisingly, is viewed as holding the solution because "[a]dvances have made vast computational power affordable and widely available, while improvements in connectivity have allowed information to be accessible in real time virtually anywhere" affording "the potential to improve health care by increasing the reach of research knowledge, providing access to clinical records when and where needed, and assisting patients and providers in managing chronic diseases." But, while policymakers are staking health care progress on big data, they seem less concerned about existential threats to the privacy of health information. The ramifications of big data are manifold. Perhaps two examples will serve to explain the thrust of this article. First, our "medical selves" exist outside of the traditional (and HIPAA/HITECH-regulated) health domain, creating exploitable confusion as our health information moves in and out of protected spaces. Second, big data positions data aggregators and miners to

perform an end-run around health care's domain-specific protections by creating medical profiles of individuals in HIPAA-free space. After all, what is the value of HIPAA/HITECH sector-specific protection designed to keep unauthorized data aggregators out of our medical records if big data mining allows the creation of surrogate profiles of our medical selves?

Summary. Terry does not expect the United States federal government to make any substantial policy changes that improve patient privacy protections. His invective is centered on the ACA, referring to it as "a hodgepodge of measures [that exist] Absent the political will to do the right thing... in today's bankrupt political climate" (p. 413). Terry asserts that even though the emergence of Electronic Medical Records (EMRs) increases the need for reformation in medical record privacy and both the Democratic and Republican parties claimed to support such reform, neither have presented strong legislation to enact such change.

Beyond his large conclusions, Terry also draws out concern for the data mining of "medically inflected data" (p. 394) – behavioral data generated in an unprotected context from which possible medical conditions can be extrapolated – allowing Big Data to "create medical records surrogates in unregulated space" (p. 405) and noting that such data "will be subject to only the lightest form of data protection" (p. 394). Terry's research is focused on patient privacy in the United States, predominantly at the federal level, in 2012. While he specifically distinguishes medically inflected data and the general privacy risks that are created by absorbing medically inflected data into Big Data, such as the scenario for fitness tracker usage, he does not delve into the possibility of employers pursuing this surrogate medical data for use in judging their employee

population. Terry intersects his analysis from legal, technological, and medical vantage points.

Terry's research is relevant for this study primarily because it establishes a clear baseline for federal inaction on the legal protection of biometric tracking data, here included in the super-category of medically inflected data. Terry recalls case law from 2011 that explicitly allows for the sale of pharmacy records as protected free speech and notes that the subsequent "data mining, therefore, is an example of widespread data aggregation and mining involving information that had its origins in information about patients" (p. 396). Terry also points out that data brokers purchase medically inflected data for their portfolios, specifically calling out how "Acxiom's own 'Consumer Data Products Catalog' lists a number of health or health-related data categories for sale" (p. 395). Terry goes on to note that other vectors for privacy protection may be available, as has been subsequently seen with the proliferation of state-level biometric privacy laws and international protections such as the GDPR. These specific examples, however, raise the possibility of inhibiting medical research being pursued for the public good.

How People Relate to Their Data and How Their Data is Understood as a Proxy for Them

Ajunwa, I., Crawford, K., & Schultz, J. (2017). Limitless worker surveillance. *California Law Review 105*(3), 735-776. https://dx.doi.org/10.15779/Z38BR8MF94

Abstract. From the Pinkerton private detectives of the 1850s, to the closed-circuit cameras and email monitoring of the 1990s, to new apps that quantify the productivity of workers, and to the collection of health data as part of workplace wellness programs, American employers have increasingly sought to track the activities of their employees. Starting with Taylorism and Fordism, American workers have become accustomed to

heightened levels of monitoring that have only been mitigated by the legal counterweight of organized unions and labor laws. Thus, along with economic and technological limits, the law has always been presumed as a constraint on these surveillance activities. Recently, technological advancements in several fields—big data analytics, communications capture, mobile device design, DNA testing, and biometrics—have dramatically expanded capacities for worker surveillance both on and off the job. While the cost of many forms of surveillance has dropped significantly, new technologies make the surveillance of workers even more convenient and accessible, and labor unions have become much less powerful in advocating for workers. The American worker must now contend with an all-seeing Argus Panoptes built from technology that allows for the trawling of employee data from the Internet and the employer collection of productivity data and health data, with the ostensible consent of the worker. This raises the question of whether the law still remains a meaningful avenue to delineate boundaries for worker surveillance. In this Article, we start from the normative viewpoint that the right to privacy is not an economic good that may be exchanged for the opportunity for employment. We then examine the effectiveness of the law as a check on intrusive worker surveillance, given recent technological innovations. In particular, we focus on two popular trends in worker tracking—productivity apps and worker wellness programs—to argue that current legal constraints are insufficient and may leave American workers at the mercy of 24/7 employer monitoring. We consider three possible approaches to remedying this deficiency of the law: (1) a comprehensive omnibus federal information privacy law, similar to approaches taken in the European Union, which would protect all individual privacy to various degrees regardless of whether or not one is

at work or elsewhere and without regard to the sensitivity of the data at issue; (2) a narrower, sector-specific Employee Privacy Protection Act (EPPA), which would focus on prohibiting specific workplace surveillance practices that extend outside of work-related locations or activities; and (3) an even narrower sector and sensitivity-specific Employee Health Information Privacy Act (EHIPA), which would protect the most sensitive type of employee data, especially those that could arguably fall outside of the Health Insurance Portability and Accountability Act's (HIPAA) jurisdiction, such as wellness and other data related to health and one's personhood.

Summary. The authors argue for the maintenance of a clear boundary between the workplace where employers have legitimate interests in surveillance and domains separate from work where the human rights to privacy and personal liberty should not be encroached upon, specifically concluding that "the freedom to safeguard one's private time and personal life should not be deemed an economic good that may be exchanged for the benefit of employment" (p. 142). This paper covers a wide spectrum of workplace surveillance mechanisms, court cases that tested the reach of those surveillance mechanisms, and regulations to prevent over-reach. The authors also include a section specific to employer-sponsored wellness programs in the United States, especially those augmented with biometric monitoring, making it particularly relevant to this study. The authors explain that "workplace wellness programs represent a $6 billion industry that includes an estimated five-hundred vendors selling programs either individually or as an optional component of healthcare insurance" (p. 130) as a contributory factor in their burgeoning popularity. Wellness program service providers can analyze employee data to offer an employer intimate information on its employees: "which prescription drugs they

use, whether they vote, and when they stop filing [*sic*] their birth control prescriptions" (p. 129).

Focusing on biometric monitoring within wellness programs, the authors note that, as with any other employer-provided device like a phone or computer, an employer-provided fitness tracker grants the employer access rights to the biometric data it collects, giving rise to privacy concerns regardless of the employer's intentions. In the authors' analysis of how biometric monitoring data from fitness trackers is opaquely analyzed for fitness programs, they signal concern over how "medical and health research rapidly changes, such that standards as to what is 'healthy' are not the same as they were in the past" (p. 132), noting that the shifting standards may be used to justify re-interpretation of individuals' seemingly-stable health. Finally, the authors note that wellness programs' focus on chronic disease prevention makes wellness programs a vector for discriminatory behavior: employees whose health data correlates with developing a disability may be targeted for elimination before the disability manifests and before anti-discrimination laws offer the employee any protection.

Becker, M. (2018, January). Understanding users' health information privacy concerns for health wearables. Presented at *The 51st Hawaii International Conference on System Sciences 2018*. Retrieved from http://toc.proceedings.com/38232webtoc.pdf

Abstract. Health information privacy concerns (HIPC) are commonly cited as primary barrier to the ongoing growth of health wearables (HW) for private users. However, little is known about the driving factors of HIPC and the nature of users' privacy perception. Seven semi-structured focus groups with current users of HWs were conducted to empirically explore factors driving users' HIPC. Based on an iterative thematic analysis

approach, where the interview codes were systematically matched with literature, I develop a thematic map that visualizes the privacy perception of HW users. In particular this map uncovers three central factors (Dilemma of Forced Acceptance, State-Trait Data Sensitivity and Transparency) on HIPC, which HW users have to deal with.

Summary. Becker used Kenny and Connolly's Health Information Privacy Concerns (HIPC) Model to engage in qualitative research with seven groups of six users of biometric trackers, specifically health wearable devices. The HIPC Model focuses on "Collection, Unauthorized Secondary Use, Improper Access, Errors, Control and Awareness" (p. 3262). The subjects who participated in this study were all voluntary consumers of this technology; none of the subjects indicated that their adoption of biometric tracking technology was incentivized by their employer or insurance plan as part of a larger wellness program. Additionally, in choosing to engage in biometric tracking, the subjects of this research determined that the benefits of the technology outweighed the perceived costs and risks to them; people who determined that costs and risks outweighed the benefits of biometric tracking were not included in this research. Becker included the following findings about consumer opinions on the use of biometric data: (a) consumers who engage in biometric tracking with wearable devices are concerned about how their biometric data is being used, (b) they only want their data to be used in ways that they have clearly agreed to, (c) they are particularly concerned with how their data is shared between corporations, (d) user satisfaction with that data-use agreement is positively correlated to their perceived control over their data. Additionally, Becker found that vendor-induced changes to terms and conditions of service reduced users' sense of control and thus satisfaction with the monitoring service; he advises

vendors to incentivize acceptance of new terms and conditions by concurrently introducing enticing new features to encourage renewed user engagement. Becker also explicitly calls out the arrival of the GDPR as a risk for service providers, but notes the transparency and control the GDPR requires for users could be marketed as features by the service provider to help reduce user privacy concerns.

This article is valuable for this study because it shows that even the consumers who freely choose to participate in biometric tracking have specific and common concerns about how their data is being collected and used that may be exacerbated in wellness programs. For example, a user may be upset by inaccurate data recording for their personal use but are substantially concerned by the possibility that their insurance company could be automatically fed inaccurate data from their biometric tracker, as wellness programs featuring biometric tracking typically are structured to do.

Crawford, K., Lingel, J., & Karppi, T. (2015). Our metrics, ourselves: A hundred years of self-tracking from the weight scale to the wrist wearable device. *European Journal of Cultural Studies 18*(4-5), 479–496. doi: 10.1177/1367549415584857

Abstract. The recent proliferation of wearable self-tracking devices intended to regulate and measure the body has brought contingent questions of controlling, accessing and interpreting personal data. Given a socio-technical context in which individuals are no longer the most authoritative source on data about themselves, wearable self-tracking technologies reflect the simultaneous commodification and knowledge-making that occurs between data and bodies. In this article, we look specifically at wearable, self-tracking devices in order to set up an analytical comparison with a key historical predecessor, the weight scale. By taking two distinct cases of self-tracking – wearables

and the weight scale – we can situate current discourses of big data within a historical framing of self-measurement and human subjectivity. While the advertising promises of both the weight scale and the wearable device emphasize self-knowledge and control through external measurement, the use of wearable data by multiple agents and institutions results in a lack of control over data by the user. In the production of self-knowledge, the wearable device is also making the user known to others, in a range of ways that can be both skewed and inaccurate. We look at the tensions surrounding these devices for questions of agency, practices of the body, and the use of wearable data by courtrooms and data science to enforce particular kinds of social and individual discipline.

Summary. Crawford, Lingel, and Karppi conclude wearable fitness trackers are an iterative development in the genealogical vein of the bathroom scale: both are marketed promising consumers enhanced knowledge of and thus control over themselves. They demonstrate that while the Quantified Self movement is a recent emergence, the rhetoric used by the Quantified Self movement has a long history. They also acknowledge that the Big Data that comes from collecting individuals' data en masse with modern fitness trackers is necessary to give meaning back to each individual because "self-tracking devices that rely on statistical comparisons are necessarily contingent on a set of data points" (p. 494). Beyond the positioning of their personal data, consumers are afforded no benefit from the wearables company's opaque Big Data: "the economic value of the data, be it for the wearables company to increase its perceived value as a big data collector or as a set to be traded and sold, is never shared with the users who make up that data set" (p. 494). This research is operating as a genealogy of self-tracking to understand how

current biometric monitoring practices with their biopolitical implications arose from the past. This genealogy starts with the publicly-available weight scale in 1885 and traces the evolution from that starting point. While there may be additional history or parallel technologies such as a thermometer, they are not included in this analysis. Additionally, while secondary effects such as playing songs are mentioned as features of the earliest public scales, the possible association with the gamification features of modern wearable self-trackers is not explored.

Crawford, Lingel, and Karppi's research is relevant for this study because in addition to being one of the core papers in this subject, they also clearly demarcate how advancing technology of self-knowledge has resulted in "a technology of *being known by others*" (p. 493-494, emphasis original). This idea is supported by citing Cigna's early move to push third-party wearable devices through an employer to insured employees. Beyond looking at how the interjection of other parties such as insurers and employers complicates the personally-focused Quantified Self, Crawford, Lingel, and Karppi also demonstrate the historical invariants in rhetoric to assist in establishing a baseline when offering the benefits of biometric tracking devices to employees.

Lupton, D. (2016). The diverse domains of quantified selves: Self-tracking modes and dataveillance. *Economy and Society 45*(1), 101-122. https://doi.org/10.1080/03085147.2016.1143726

Abstract. The concept of self-tracking has recently begun to emerge in discussions of ways in which people can record specific features of their lives, often using digital technologies, to monitor, evaluate and optimize themselves. There is evidence that the personal data that are generated by the digital surveillance of individuals (dataveillance)

are now used by a range of actors and agencies in diverse contexts. This paper examines the ‘function creep’ of self-tracking by outlining five modes that have emerged: private, communal, pushed, imposed and exploited. The analysis draws upon theoretical perspectives on concepts of selfhood, citizenship, dataveillance and the global digital data economy in discussing the wider socio-cultural implications of the emergence and development of these modes of self-tracking.

Summary. This article depicts five non-exclusive, intersecting modes of self-tracking: private, pushed, communal, imposed, and exploited. When self-tracking "is undertaken for purely personal reasons, and the data are kept private or shared with limited and select others" (p. 105), it is considered to be *private*. *Pushed* self-tracking features an "initial incentive for engaging in dataveillance of the self [that] comes from another actor or agency" (p. 106). *Communal* self-tracking describes collective sharing of self-tracking results, such as the Quantified Self community engages in. *Imposed* self-tracking occurs in contexts where individuals cannot simply opt-out of dataveillance, commonly in workplaces and schools. Finally, *exploited* self-tracking occurs when the data that was collected from another mode of self-tracking is "repurposed for the financial benefit of others" (p. 111).

Lupton then pivots to consider how "lively data and data practices" (p. 114) are connected larger issues of "digital biocapital and data politics" (p. 116), noting that sending self-tracking data to the internet generally leads to some degree of exploitation of that data in ways that cannot be undone. "Given the ways in which digital data are generated, stored, managed and used, once they are digitized, the array of practices that began as personal and private tend to become inextricably imbricated within these

networks and economies" (p. 114-115). Lupton concludes that the design of self-tracking conforms to a political agenda in which citizens engage in "self-responsibilized practices of dataveillance and life optimization and emitting valuable ‘data exhausts’ for repurposing by other actors and agencies" (p. 118), but that exploitation is not the predetermined outcome of self-tracking.

Lupton engages in substantial abstraction; the article is not focused on any particular location, relationship, or means of self-tracking. Lupton’s approach is intentional, as he is working to describe major trends. Lupton does specifically reference biometric tracking in employer-sponsored wellness programs, however, noting that "These programmes are found particularly in the United States, where employers pay for health insurance coverage for their employees, and it is therefore in their financial interests to promote good health among their workers" (p. 108).

Overall, this article adds to this study in two important ways. First, it provides a framework for understanding how individuals understand being enjoined to the practice of self-tracking: while workplace incentives suggest that the employer-sponsored wellness program is engaging in pushed self-tracking, there are alternative modes of self-tracking that employers may engage in or avoid to manage employee perception of self-tracking in the workplace. Second, the discussion of data on a network taking on a life of its own is a crucial reminder that the data will persist long after the employer-provided incentive for participation is gone. "This vitality of data has significant implications for how self-trackers use and share their data with others on social media and also for how they may lose control of their data as they enter the digital data economy " (p. 114) and

when control over the data is lost, the data can then be repurposed for adversarial use against the employee or their employer.

Ruckenstein, M. & Schüll, N. (2017). The datafication of health. *Annual Review of Anthropology 46,* 261-278. https://doi.org/10.1146/annurev-anthro-102116-041244

Abstract. Over the past decade, data-intensive logics and practices have come to affect domains of contemporary life ranging from marketing and policy making to entertainment and education; at every turn, there is evidence of "datafication" or the conversion of qualitative aspects of life into quantified data. The datafication of health unfolds on a number of different scales and registers, including data-driven medical research and public health infrastructures, clinical health care, and self-care practices. For the purposes of this review, we focus mainly on the latter two domains, examining how scholars in anthropology, sociology, science and technology studies, and media and communication studies have begun to explore the datafication of clinical and self-care practices. We identify the dominant themes and questions, methodological approaches, and analytical resources of this emerging literature, parsing these under three headings: datafied power, living with data, and data–human mediations. We conclude by urging scholars to pay closer attention to how datafication is unfolding on the "other side" of various digital divides (e.g., financial, technological, geographic), to experiment with applied forms of research and data activism, and to probe links to areas of datafication that are not explicitly related to health.

Summary. Ruckenstein and Schüll conclude that in addition to the asymmetry between the biometric monitoring device companies compiling the Big Data and the individuals generating the data, there is another divide between the individuals who are included and

the unrepresented individuals – often the unemployed or unindustrialized. The authors assert that the inclusion of the unrepresented is necessary to create a complete understanding of human health. They further conclude that individual and collective data activism is necessary to "reappropriate and rearticulate concepts such as 'sharing' and 'the public good' that have been co-opted by technology companies seeking free access to their users' data" (p. 272). Finally, they conclude with a concern that the datafication of health is blurring the boundaries between health and other domains, particularly finance, in ways that redefine what it means to be healthy. The authors note that emerging literature on health datafication focuses on "North America, the United Kingdom, Australia, and Northern Europe" (p. 262) where internet adoption intersects with instability in healthcare systems. This set of subjects is broader than the typical focus on employers in the United States, but could emerge as a limit for multinational corporations pursuing a global roll-out of wellness programs. The authors mention that much of the literature is based on Foucault's analysis of surveillance in a disciplinary society, but they engage with an emerging trend of analyzing dataveillance, where many different parties are collecting and aggregating partial information about subjects, which matches the multi-agent set of relations involved in employer-sponsored insurance with wellness programs that feature biometric tracking devices.

The authors' focus on the asymmetric nature of Big Data when applied to wellness programs justifies taking extra care in the design of data collection and processing approaches in this context: "Health data streams can become part of a multitude of different agendas, each wanting to assert its particular script for coding, protecting, and modifying health" (p. 270). The authors also note that the immediate corporate goals of

the wellness program are not the only ones being pursued. Furthermore, there is a "volatile range of affective orientations that people have toward the tracking of self-data" (p. 267) that needs to be considered when presenting a tracking-enhanced wellness program to a diverse employee population.

Slomovic, A. (2017). eHealth and privacy in U.S. employer wellness programs. In R. Leenes, N. Purtova, & S. Adams (Eds.), *Under Observation: The Interplay between eHealth and Surveillance* (pp. 31-58). Switzerland: Springer. Doi: 10.1007/978-3-319-48342-9 Retrieved from https://ssrn.com/abstract=2613452

Abstract. This paper summarizes privacy, autonomy and ethical issues raised by employer-sponsored wellness programs in the United States, with emphasis on the increasing use of technology for collecting data and shaping participant behavior. After providing some background on wellness programs, the paper looks at the types of personal information collected in these programs through health risks assessments, biometric screenings and, increasingly, wearable fitness trackers and mobile apps, at ways in which this personal information is combined with public data and healthcare data, and how it is used to monitor and influence program participants. The paper examines legal protections available to employees in areas of informational privacy, physical integrity, and decisional autonomy. It concludes with recommendations for further research.

Summary. This article raises three contested claims about employer-sponsored wellness programs and offers four policy-oriented recommendations to address them. The first contested point is whether employee participation in wellness programs is voluntary. Slomovic noted that 40 percent of employees participating in a wellness program

reported that they felt like they were forced to do so, with the intrusiveness of the programs resulting in reduced morale. Second, it is not clear that wellness programs improve health outcomes and lower costs; Slomovic reported that some of "these programs lead to overtesting, overdiagnosis, and overtreatment, all of which carry their own health risks and increase healthcare costs" (p. 18) and appear counterproductive to the health care cost reduction goals of the wellness program. Finally, in addressing the possibility of principled resistance against data expropriation by means of submitting disinformation, Slomovic raises the concern that there is no clear distinction between employees who use disinformation as resistance and employees who are merely lying to cheat the system.

Concluding that the United States is likely to continue using employer-provided health insurance for the foreseeable future, Slomovic recommends mapping the commercial ecosystem of wellness data, passing legislation regulations to protect the data and the participants providing the data, limiting the use of incentives attached to wellness programs beyond the premium discounts specified by the ACA, and establishing institutional review boards to prevent overcollection and misuse of data.

This article's survey of employer-sponsored wellness programs in the United States as biometric monitoring was beginning to appear as a feature of the programs provides relevant findings related to the purpose of this paper. The notable limitation of the article is that Slomovic raises the concern of overtesting leading to counterproductive overdiagnosis and overtreatment, but does not call for those employer-facing costs to be analyzed as part of the wellness program's total costs, choosing to instead look at the concern through an ethical lens of new interests invading a space of doctor-patient

privilege. Overall, this article is relevant to this paper specifically for the three contested claims raised by Slomovic as they each demonstrate that choices made in wellness program design will alter the outcomes it produces, both directly and indirectly.

Smith, G. (2016). Surveillance, data and embodiment: On the work of being watched. *Body & Society 22*(2). 108-139. doi: 10.1177/1357034X15623622

Abstract. This paper proposes the analytics ‘disembodied exhaust’ and ‘embodied exhaustion’ to conceptualize processes of bodily datafication in the ‘networked age’. As the body interfaces with networked media technologies and infrastructures, it emits disembodied exhaust which comes to establish a parasitic data-proxy. It is this networked actant that progressively mediates how embodied subjects experience their daily lives. Care must be thus exercised in terms of its stylization. The paper explicates the character and function of the data-proxy in today's personal information economies and it conceptualizes the symbiont nature of the encounter between data-providers and their networked selves. It suggests that managing a protrusive data-proxy is akin to a work relation, demanding the investment of energy, expertise, foresight and resource. But it also shows how this actant troubles popular binary distinctions of agency and actancy, mortality and immortality, presence and absence.

Summary. This article investigates how people comprehend the difference between their experience of their body and behaviors and the data that is sensed and collected from their body as exhaust from their behaviors. Smith depicts people as *technovisuals*: “those who act with technology and are consequently visualised by it” (p. 110). The investigation arose from the concern that a person's collected data exhaust will subsequently be used as a proxy for them and can alter "social relations in ways that often

bypass the awareness, let alone influence, of its embodied referent" (p. 134). Despite the lack of specific awareness of how an individual's data-proxy is being used, asymmetric power relations insist that the individual is responsible for the accuracy of their data-proxy. "The responsibility for conserving the content and for anticipating the probable uses and effects of disembodied exhaust progressively falls on the exposed technovisual" (p. 134). Smith argues that awareness of this responsibility results in the individual experiencing "performative fatigue that accompany the experience of data-based visibility" (p. 135); in other words, maintaining the attractiveness of one's data-proxy can be hard work. The article notes how this individual responsibility is complicated by "the spread of networked sensor technologies" (p. 111) that result in personal information being leaked into collections where it is indefinitely available for recall.

The article introduces a framework for engaging with the human experience and maintenance of datafication, particularly to address gaps in legacy surveillance studies that technological advancements have opened up. While this article does not focus on wellness programs or biometric monitoring as use cases, it allows for the placement of the employer-sponsored wellness program and biometric monitoring in a larger context of how people outside of an employer/employee relationship are subjected to digital visibility in modern social life. Smith grants that he does not investigate nuanced differences in reactive behaviors correlating to social markers like ethnicity, age, or gender; the persons described by the article are abstracted and impersonal. This article is still valuable to this study because it looks at the work people put into nourishing their "parasitic data-proxy" (p. 125) outside of any granular relationship to an employer or an

insurer, providing a context for understanding that people will bring their pre-established behavioral patterns to their employer's wellness program.

Challenges and Shortcomings in Converting Complex Wellness Programs Into Positive Health Outcomes

Christophersen M., Mørck P., Langhoff T.O., Bjørn P. (2015) Unforeseen challenges: Adopting wearable health data tracking devices to reduce health insurance costs in organizations. In M. Antona & C. Stephanidis (Eds.), *Universal access in human-computer interaction. Access to learning, health and well-being: 9th international conference, UAHCI 2015* (pp. 288-299). Switzerland: Springer, Cham. https://doi.org/10.1007/978-3-319-20684-4_28

Abstract. Wearable health-tracking devices are being adopted by American self-insured companies to combat rising health insurance costs. The key motivation is to discourage employees' unhealthy behavior through monitoring their data. While wearable health-tracking devices might improve users awareness about personal health, we argue that the introduction of such devices in organizational settings also risk introducing unforeseen challenges. In this paper we unpack the unforeseen challenges and argue that wearable health-tracking devices in organizational settings risk disciplining employees, by tempting or penalizing them financially. Further, health concerns are reduced to numbers through wearable health-tracking devices providing surveillance of bodies, impacting people's lives. We stress how important it is that designers and researchers find ways to address these challenges in order to avoid future abuse of personal health data collected from wearable health-data tracking devices.

Summary. This article investigates several ways in which the use of biometric tracking can fail to result in positive health outcomes, both at personal and societal levels. Focusing on private health insurance in the United States, the authors conclude that "the integrity and validity of this health data can be compromised through the lack of standards, context and manipulation leading to wrongly determined insurance premiums" (p. 297). This is not just a short-term concern; submitting to biometric tracking "may affect future insurance options and prices, even if annulled, because the data has already become part of the digital health sets [*sic*] immortal memory" (p. 296). The article is the distillation of challenges discovered across 28 data sources through a grounded theory approach; Christophersen et al. found common challenges around data ownership, security, and privacy; interpreting data with regards to context and manipulation; and business and insurer goals of minimizing risk, differentiating pricing, preventing opt-outs, and dictating user behavior. While the authors stop short of suggesting remedial actions to address the challenges thye describe, the article is still well-suited to this study due to its heavy focus on employer-sponsored wellness programs as a locus for engaging individuals with biometric measurements, from routine screenings to active tracking, at the behest of insurance companies. This article is additionally valuable for this study because it raises two particular concerns in tandem: appearance and time. It specifically explains that "health insurance premiums of individuals are differentiated in price based on whether or not healthy *looking* [emphasis added] data can be provided" (p. 297), exposing the incentive for the insured individuals to manipulate the data being provided to their insurers. This manipulation will in turn be countered by the insurers' need to maintain both their profits and their customer incentives; in reaction to an increasingly

healthy-looking data set, "the health boundaries defining what is natural could quickly be remade to be unnatural" (p. 296-297) simply by adjusting the interpretation of which numbers seem to be indicative of good health. Christopherson et al. assert that the perpetually updated interpretations of health and risk derived from the ongoing analysis of Big Data collected from biometric monitoring will continually allow insurance companies to update their premiums, specifically increasing them on marginal populations as a means of accounting for newly-discovered risks regardless of the actual health outcomes of the populous at large. The authors put it bluntly by stating the profit motive for insurers necessitates depicting their customers as a "herd of unfit cyborgs" (p. 297).

Jones, D., Molitor, D., Reif, J. (2018). *What do workplace wellness programs do? Evidence from the Illinois workplace wellness study*. Cambridge, MA: National Bureau of Economic Research. Retrieved from https://www.nber.org/papers/w24229.pdf

Abstract. Workplace wellness programs cover over 50 million workers and are intended to reduce medical spending, increase productivity, and improve well-being. Yet, limited evidence exists to support these claims. We designed and implemented a comprehensive workplace wellness program for a large employer with over 12,000 employees, and randomly assigned program eligibility and financial incentives at the individual level. Over 56 percent of eligible (treatment group) employees participated in the program. We find strong patterns of selection: during the year prior to the intervention, program participants had lower medical expenditures and healthier behaviors than non-participants. However, we do not find significant causal effects of treatment on total medical expenditures, health behaviors, employee productivity, or self-reported health

status in the first year. Our 95% confidence intervals rule out 83 percent of previous estimates on medical spending and absenteeism. Our selection results suggest these programs may act as a screening mechanism: even in the absence of any direct savings, differential recruitment or retention of lower-cost participants could result in net savings for employers.

Summary. This freshly-concluded year of primary research actively contradicts older research from 2010 that found that employee wellness programs led to substantial health care saving. Its scope was also limited to Illinois, one of the states with enhanced legal protection for biometric data, specifically centered on the University of Illinois at Urbana-Champaign. It focused on the effects of wellness programs featuring one-time biometric screenings and organized activities, but did not explore potential additional effects of biometric trackers. The authors' experimental framework randomly distributed participants across one control group and six treatment groups, testing "for the joint equality of the seven coefficients" as well as estimating "a seemingly unrelated regression model to test whether the variables listed within each panel predict enrollment into either the control or any of the six treatment groups" (p. 15). Additionally, the authors assert that a “unique feature of our study is our ability to characterize the employees who declined to participate in our experiment” (p. 15).

The authors conclude that there are no direct significant financial benefits that occur from a wellness program over the course of a year, contradicting earlier findings that helped to popularize wellness programs. The authors’ investigation into wellness plan participation does find that "non-participating employees are more likely to be in the bottom quartile of the salary distribution, are less likely to engage in healthy behaviors, and have higher

medical spending, on average" (p. 6) and suggest that if they could increase participation by 4.5 percent then "this change in composition alone would offset the entire costs of our intervention" (p. 4). However, lacking research into the feasibility of such a shift, the authors assert that "this calculation does not imply that adoption of workplace wellness programs is socially beneficial" (p. 26). Overall, they find that selection biases in "workplace wellness programs shift costs onto low-income employees" (p. 33). They grant that a single-year study may be inadequate to fully understand results, but note that "if there is sufficient employee turnover then these benefits may not accrue to the employer who made the initial investment in workplace wellness" (p. 33).

This experimental research is relevant to this study in three ways. First, they find a selection bias that results in the self-exclusion of low-income employees who tend to be in poorer health or have worse health habits than other employees. Second, the authors raise the possibility that the lack of positive outcomes for participants are because they are simply "earning rewards for behaviors they already enjoy" (p. 1). Third, the results of this experiment indicate that if the success of a corporate wellness program is going to be judged by its return on investment, then it needs to actively entice the "low-income employees with high health care spending and poor health habits" (p. 33) to participate rather than just shifting costs onto them for non-participation.

Hull, G. & Pasquale, F. (2018). Toward a critical theory of corporate wellness. *BioSocieties13*(1), 190-212. Retrieved from: https://ssrn.com/abstract=3010313

Abstract. In the U.S., ‘employee wellness’ programs are increasingly attached to employer-provided health insurance. These programs attempt to nudge employees, sometimes quite forcefully, into healthy behaviors such as smoking cessation and

exercise routines. Despite being widely promoted as saving on healthcare costs, numerous studies undermine this rationale. After documenting the programs' failure to deliver a positive return on investment, we analyze them as instead providing an opportunity for employers to exercise increasing control over their employees. Based on human capital theory and neoliberal models of subjectivity that emphasize personal control and responsibility, these programs treat wellness as a lifestyle that employees must be cajoled into adopting, extending the workplace not just into the home but into the bodies of workers, and entrenching the view that one belongs to one's workplace. At the same time, their selective endorsement of health programs (many scientifically unsupported) produce a social truth of wellness framed as fitness for work. We conclude by arguing that the public health initiatives occluded by the private sector's promotion of wellness programs would be a much better investment of resources.

Summary. Hull and Pasquale find that employer-sponsored wellness programs are based on an understanding of health insurance as a moral hazard and a desire to shift responsibility for health onto the workers "with no attention paid to the larger environment that created many of the risks that workers are told to avoid" (p. 28). But since health insurance can also be a way to diffuse risk, the expectation of health insurance operating as a moral hazard results in wellness programs having unreliable results. This exposes the promise of positive health outcomes from wellness programs as a rationalization for entrenching the power relations between employer and employees. Hull and Pasquale finally conclude that companies wanting to save money on health insurance should be lobbying for public health programs, and that any continuing wellness programs should be informed by employee input. The authors do grant that

wellness programs targeting smoking cessation and preventing or managing chronic disease, specifically diabetes (p. 19), can be reliably positive for both employer and employees. The bulk of their argument, however, is that the breadth of wellness programs has been over-reaching into employees' lives for 30 years compared to the narrow instances where their interventions are valuable. Hull and Pasquale use a split perspective on health insurance, comparing its capacity for risk-spreading to its tendency for moral hazard, specifically linking the view of insurance as a moral hazard to neoliberalism. The continual isolation of personal choices is used to frame their alternative view on wellness programs.

This article is relevant for this study because the authors critique the framework of the proposition that wellness programs and biometric tracking are necessary to promote employee well-being. Contrary to the trend of increasing complexity in workplace wellness programs and their expansion into biometric monitoring, Hull and Pasquale argue that such programs do not ensure better employee health and that simple programs targeting easily measured high-value outcomes would be ethically preferable within the existing employer-sponsored health insurance framework.

Finally, but critically when extending this research, Hull and Pasquale cite research such as Ferrie et al. (2016) that "suggested causal links between employee feelings of job insecurity and both diabetes and incident coronary heart disease" (p. 21), indicating that even if an employer’s legitimate desire to lower health care spending is animating their push for a wellness program, auditing and adjusting the corporate culture to create a healthier physiological environment for employees may be more cost-effective than implementing a wellness program.

Oravec, J. A. (2018). Intimate infiltrators: Ethical issues in the integration of self-tracking practices into workplace contexts. Presented at *International Association for Media and Communication Research Conference 2018*.

Abstract. This paper aims to address the ethical dimensions of the complex and evolving relationships between individuals and self-tracking devices in workplace systems, mapping how the interactions involved can affect the quality of data produced (and the related medical research efforts) as well as the wellbeing, security, and privacy of participants. It explores the notion of "pushed" medical self-tracking devices and examines how the protection of "mental and physical integrity" can be applied in analysis of the activities of employees using such devices. Special concerns arise when such potentially-stigmatizing information as employee weight and menstrual cycles are tracked. The dystopian images of (1) organizations developing their operations to produce optimal quantities of health-related data (data "farming" that is undertaken with little consideration of the better interests of the employees involved), and (2) the workplace as a system designed to "groom" specific employee physical and mental characteristics and routines, can readily emerge from these analyses. Individuals' capacities to make valid medical decisions concerning their use of the devices can be diminished by the addictive and gamified aspects of the systems or through the rhetorical promotion of specific philanthropic or health-themed objectives; the anxieties and addiction involve may serve to compound other forms of workplace stress and impact employees' compliance with organizational control systems. The paper also explores how various emerging employee-initiated activities (such as the manipulation and gaming of device-produced data) can be aspects of user resistance. These possibly-subversive

activities can have influences on medical data analyses as well as the usefulness of the data produced for subsequent profiling and criminal investigation efforts by organizations but also introduce some level of freedom of expression into otherwise intrusive systems.

Summary. Oravec is concerned that biometric monitoring in workplace wellness programs is "utilized in data production efforts rather than involved in authentic health maintenance efforts" (p. 11) and depicts multiple hypothetical scenarios of how employers could use employee biometric data for discriminatory purposes. Oravec suggests these potential abuses risk undermining positive and legitimate uses for biometric tracking technologies. Oravec draws on research showing that employees rationalize heightened levels of manipulation, abuse, and abandonment of biometric monitoring devices specifically associated with their workplace or employer, undermining the validity of the data set. Oravec also makes note of the layered asymmetry in the use of the data: employees having biometric data collected from them have little recourse in addressing abuses of the data by any of the several organizations involved in the process. Finally, Oravec argues that compelling employees to engage in the cognitive labor of being observed is ethically treacherous territory that requires monitoring. She compounds this point with a review of contest- and lottery-style incentive programs that were found to be counterproductively linked to anxiety-related and addictive behaviors.

Oravec's immediate-future vision, building on a broad base of research, was the starting point for this paper and thus fits within the scope of the problem, but this article faces a couple of limitations; it does not examine the momentum behind workplace wellness programs that drive organizations to adopt them, nor does it actually suggest practices

that could improve employee health outcomes. Overall, this article is critical for this paper because it directly calls out the need for employers to work on "mitigating the 'creepy' factor" (p. 9) of wellness programs that include biometric tracking, noting that the good intentions that introduce a wellness program will not curb the potential abuse of employee data, and an employer marketing the changes to their health program as empowering will not conceal the forced acceptance of those changes facilitated by asymmetric power relations between employer and employees.

Till, C. (2014). Exercise as labour: Quantified Self and the transformation of exercise into labour. *Societies 2014*(4), 446-462. doi:10.3390/soc4030446

Abstract. The recent increase in the use of digital self-tracking devices has given rise to a range of relations to the self often discussed as quantified self (QS). In popular and academic discourse, this development has been discussed variously as a form of narcissistic self-involvement, an advanced expression of panoptical self-surveillance and a potential new dawn for e-health. This article proposes a previously un-theorised consequence of this large-scale observation and analysis of human behaviour; that exercise activity is in the process of being reconfigured as labour. QS will be briefly introduced, and reflected on, subsequently considering some of its key aspects in relation to how these have so far been interpreted and analysed in academic literature. Secondly, the analysis of scholars of “digital labour” and “immaterial labour” will be considered, which will be discussed in relation to what its analysis of the transformations of work in contemporary advanced capitalism can offer to an interpretation of the promotion and management of the self-tracking of exercise activities. Building on this analysis, it will be proposed that a thermodynamic model of the exploitation of potential energy underlies

the interest that corporations have shown in self-tracking and that "gamification" and the promotion of an entrepreneurial selfhood is the ideological frame that informs the strategy through which labour value is extracted without payment. Finally, the potential theoretical and political consequences of these insights will be considered.

Summary. Till concludes that the creation of valuable biometric data by means of self-tracking while exercising results in the exercise constituting labor. It notes that the accumulation of that data allows a third party to extract value from it, as is structurally consistent with Marxist analysis. The core of the argument is that even immaterial and gamified activity constitutes labor when value is extracted from the result by a third party, but that the third party extracting the value has an interest in not recognizing the contributory labor. While this article recognizes the directives of corporate wellness programs, its vision is limited to proving the economic viability of generated data so it settles for focusing on using the data for advertising. This limitation is perhaps due to the article being written before biometric trackers were a popular addition to employer-sponsored wellness programs – the author indicates that the epistemic changes in extracting value from self-tracking data were in their early stages at the time of publication – but the slight attention to private insurance interests could also be the result of the author's use of the United Kingdom as an immediate frame of reference.

This article contributes three elements to this study. First, it reiterates the commercial viability of a data set of accumulated self-tracking data beyond the original data collector's purpose. Second, it provides a critical framework for understanding labor and recognizing the existence of immaterial labor and knowledge work in the modern economy. Finally and most importantly, Till connects the use of biometric monitoring in

the workplace with the use of biometric monitoring as part of an employer-sponsored wellness program that is intended to reduce health insurance spending for the employer to show the lack of distinction between labor that the employer is or is not paying wages for, noting a growing fusion of time across the boundaries of work and leisure.

Conclusion

The content of this literature review includes the challenges for employers in the United States with establishing or augmenting a workplace wellness program with biometric monitoring, such as a fitness tracker (Claxton et al., 2018). Following the policy guidance of the ACA, a variety workplace wellness programs have grown from commonplace to pervasive among large employers (Mattke et al., 2013), driven by hundreds of consulting vendors (Ajunwa et al., 2017). A growing trend among these workplace wellness programs is to provide biometric monitoring, such as a fitness tracker, to employees so they can have and offer their employers confirmation of their good health habits and progress towards fitness goals, potentially earning discounts on insurance premiums or being entered into contests for prizes (Ajunwa et al., 2017; Claxton et al., 2018; Hull & Pasquale, 2018; Jones et al., 2018; Lupton, 2016; Oravec, 2018; Ruckenstein & Schüll, 2017). The literature warns of numerous difficulties that can arise, including: (a) lack of employee engagement (Fronstin & Roebuck, 2015), (b) errant data collection, either due to inaccurate sensors or intentional employee misuse of their biometric monitors (Becker, 2018; Oravec, 2018), (c) misuse of employees' medically inflected data by the employer or third parties that collect or subsequently purchase the data (Terry, 2012), and (d) employees regarding the process of data collection as employer-compelled labor (Smith, 2016; Till, 2014). In addition to the many potential issues that may arise with the use of employer-sponsored biometric monitors, workplace wellness programs have been woefully inconsistent in generating positive results for both employers and employees (Hull & Pasquale, 2018).

These challenges are side-effects to problems of control: users expect personal biometric monitoring technology to empower them with greater control over their bodies by means of personal quantification (Crawford et al., 2015; Lupton, 2016), but are reticent to lose control of

the numbers their bodies produce to outside parties (Becker, 2018; Lupton, 20016; Ruckenstein & Schüll, 2017). Looking to Lupton's (2016) depictions of modes of self-tracking, a lack of personal control is present in the modes of imposed and exploited self-tracking. As such, workplace wellness programs should be designed to avoid those modes of self-tracking.

Avoiding the mode of imposed self-tracking is not merely a matter of having a voluntary program, as Slomovic (2017) found that 40 percent of participants in wellness programs felt that their involvement was compulsory despite legal requirements that participation in workplace wellness programs be voluntary. While workplace wellness programs that feature biometric monitoring are always going to engage in pushed self-tracking, careful design of incentives is needed to attract employees who would benefit from the program instead of simply rewarding already-healthy employees for doing more of what they enjoy (Jones et al., 2018). Although fiscal incentives are both common and useful for increasing participation, they should not be deployed arbitrarily or relied upon exclusively for driving engagement (Claxton et al., 2018; Fronstin & Roebuck, 2015). Fronstin and Roebuck (2015) specifically disclaim the fiscal incentives they were studying as the sole driver of increased employee participation, noting that "increased member-communication efforts that reached all employees may have contributed to these higher participation rates" (p. 16). Borrowing from the community structure of the Quantified Self movement (Crawford et al., 2015; Lupton, 2016; Ruckenstein & Schüll, 2017), it can be inferred than an employer might also try to activate the mode of communal self-tracking by providing mild support to an employee group focused on healthy living, with that group providing a broad base of peer influence to nudge other employees into wellness program participation.

Addressing employees' health information privacy concerns is crucial to mitigating their resistance to biometric monitoring as part of workplace wellness programs (Becker, 2018; Lupton, 2016; Ruckenstein & Schüll, 2017). Workplace wellness programs with biometric monitoring can be readily abused by employers (Hull & Pasquale, 2018; & Oravec, 2018), and the data collected from biometric monitoring can be exploited by insurance companies to maintain ongoing profitability (Christophersen et al., 2015), as self-tracking consumers are already savvy enough to realize independently (Becker, 2018). The purpose of data retention is to have data when future analytical uses are discovered for it (Foucault, 1977), and a crucial part of the phenomenon of Big Data is discovering novel ways to produce new truths from existing data (boyd & Crawford, 2012). The use of Big Data to continually produce new truths about health allows for ongoing redefinitions of what constitutes a health risk, concurrently discovering and potentially exposing a population that appears vulnerable to the newly-declared risk (Ajunwa et al., 2017; Christopherson et al., 2015). In order to address the common health information privacy concerns Becker (2018) detailed, it is thus important to explain to employees both how the biometric data they generate will initially be used as well as describing the restrictions and protections that prevent subsequent data misuse, both by the employer and by third-parties.

The other crucial element of communication around workplace wellness programs is what they are intended to do and subsequently determining whether they are successful. Many wellness programs do not get formally evaluated for efficacy against goals (Mattke et al., 2013), or change their goals and avoid accountability for specific outcomes (Hull & Pasquale, 2018). Workplace wellness programs that routinely generate positive outcomes focus on high-value targets such as smoking cessation and diabetes management (Hull & Pasquale, 2018). The longer-term effects of preventative pharmacotherapy on employee health, as Fronstin and

Roebuck (2015) correlated with participation in workplace wellness programs, complicates evaluation: a program that regards prescription drug usage as a sign of success is likely to nudge healthy participants into the overdiagnosis and overtreatment correlated with workplace wellness programs (Slomovic, 2017). By choosing to focus a wellness program on specific high-value targets, the data collection from employees can be shaped to also focus on those targets (Ruckenstein & Schüll, 2017) to limit possibilities for exploited self-tracking: a program focused on helping employees manage diabetes can exclude other sensitive data about their sexuality (Ajunwa et al., 2017; Oravec, 2018), for example. Ultimately, a workplace wellness program should have goals and a timeline and be held accountable for them to justify the collection of intimate biometric data from employees (Ajunwa, 2019).

Working as peer corporations with service providers to limit the third-party exploitation of biometric data is also action an employer could take on behalf of its employees to limit the proliferation of third-party agendas described by Ruckenstein and Schüll (2017). The shortage of consumer-grade biometric monitors that are fully GDPR-compliant in giving their users control of personal medically-inflected data (Becker, 2018; Fietkiewicz & Henkel, 2018) indicates a market opportunity that other large employers or insurers could use as a condition of bulk-purchasing. Lacking contractual assurances from biometric monitoring service providers, employers should reconsider providing an incentive for participation in ongoing biometric monitoring of employees; while the employer may be seen as by their employees as compelling labor that generates and harvests the employees' biocapital (Smith, 2016; Till, 2014), the employer is not the primary beneficiary of the resulting data set (Crawford et al. 2015; Ruckenstein & Schüll, 2017; Smith, 2016; Till, 2014). While Slomovic (2015) took issue with unconventional incentives outside of fiscal boundaries, one suggestion should an employer be

unable to defend its employees' privacy but still want to promote good health habits is for the employer to instead consider offering the biometric monitoring devices as incentive gifts for participating in other workplace wellness initiatives, such as an annual preventative biometric screening or physician-administered physical, without engaging in ongoing data collection from the devices for the wellness program. While this approach does not completely resolve the possibility of third-party data exploitation, it does prevent many of the most direct employer- and insurer-linked scenarios for data overreach from manifesting (Ajunwa et al., 2017; Becker, 2018; Oravec, 2018). Any employee who cares to engage in self-quantification as a means to self-management as has been common for generations (Crawford et al., 2015) has the opportunity to use the gift appropriately to improve health habits, as was likely the intent of the workplace wellness program in the first place (Mattke et al., 2013).

Going forward, the impact of expansive new consumer protection and privacy regulations such as the GDPR may change the business models and data retention risk tolerance currently formalized by health insurers and biometric monitoring service providers (Pearlman et al., 2017; Wachter, 2018). Ajunwa (2019) and Fietkiewicz and Henkel (2018) are already producing fresh work in this space, but the breadth of regulation that organizations can be exposed to when considering global business models and local ordinances suggests that there will be a surplus of regulatory and case law material to be reviewed and analyzed to help guide legal compliance for some time to come.

References

Ajunwa, I., Crawford, K., & Schultz, J. (2017). Limitless worker surveillance. *California Law Review 105*(3), 735-776. https://dx.doi.org/10.15779/Z38BR8MF94

Ajunwa, I. (2019). Algorithms at work: Productivity monitoring platforms and wearable technology as the new data-centric research agenda for employment and labor law. *St. Louis University. Law Journal 63 (forthcoming)*. Retrieved from https://ssrn.com/abstract=3247286

Andrejevic M. (2014). The big data divide. *International Journal of Communication 8*, 1673–89. Retrieved from https://ijoc.org/index.php/ijoc/article/view/2161/1163

Becker, M. (2018, January). Understanding users' health information privacy concerns for health wearables. Presented at *Hawaii International Conference on System Sciences 2018*. Retrieved from http://hdl.handle.net/10125/50301

Binns, R., & Bietti, E. (2018, October 18). Acquisitions in the third party tracking industry: competition and data protection aspects. *SSRN*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3269473

boyd, d. & Crawford, K. (2012) Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication & Society 15*(5). 662-679. https://doi.org/10.1080/1369118X.2012.678878

Center for Public Issues Education. (n.d.). Evaluating information sources. *University of Florida Institute of Food and Agricultural Studies*. Retrieved on November 16, 2018 from https://canvas.uoregon.edu/courses/120122/files/5706985/download?wrap=1

Christophersen M., Mørck P., Langhoff T.O., Bjørn P. (2015) Unforeseen challenges: Adopting wearable health data tracking devices to reduce health insurance costs in organizations. In

M. Antona & C. Stephanidis (Eds.), *Universal access in human-computer interaction. Access to learning, health and well-being: 9th international conference, UAHCI 2015, held as part of HCI International 2015, Los Angeles, CA, USA, August 2-7, 2015, proceedings, part 3*. *Lecture notes in computer science, vol 9177* (288-299). Switzerland: Springer, Cham. https://doi.org/10.1007/978-3-319-20684-4_28

Chun, W. H. K. (2016). *Updating to remain the same: Habitual new media*. Cambridge, MA: MIT Press.

Claxton, G., Rae, M., Long, M., Damico, A., & Whitmore, H. (2018). Kaiser family foundation employer health benefits 2018 annual survey. *Henry J. Kaiser Family Foundation*. Retrieved from http://files.kff.org/attachment/Report-Employer-Health-Benefits-Annual-Survey-2018

Crawford, K., Lingel, J., Karppi, T. (2015). Our metrics, ourselves: A hundred years of self-tracking from the weight scale to the wrist wearable device. *European Journal of Cultural Studies 18*(4-5), 479-496. doi:10.1177/1367549415584857

Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor.* New York, NY: St. Martin's Press.

Ferrie, J., Virtanen, M., Jokela, M., Madsen, I., Heikkilä, K., Alfredsson, L., ... Kivimäki, M. (2016). Job insecurity and risk of diabetes: A meta-analysis of individual participant data. *Canadian Medical Association Journal 188*(17-18). doi: 10.1503/cmaj.150942

Ferryman, K. (2017, April 21). Reframing data as a gift. Presented at *2017 Sage Assembly*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3000631

Fietkiewicz, K.J., Henkel, M. (2018) Privacy protecting fitness trackers: An oxymoron or soon to be reality?. In G. Meiselwitz (Ed.), *Social computing and social media. User experience*

and behavior. SCSM 2018. Lecture notes in computer science, vol 10913 (431-444). Switzerland: Springer, Cham. https://doi.org/10.1007/978-3-319-91521-0_31

Foucault, M. (1977). *Discipline and punish: The birth of the prison* (A. Sheridan, Trans.). New York: Vintage Books.

Foucault, M. (1985). *The use of pleasure* (R. Hurley, Trans.). New York: Vintage Books.

Henry J. Kaiser Family Foundation. (2017), The uninsured: A primer - Key facts about health insurance and the uninsured in the era of health reform: Supplemental Tables. Retrieved from http://files.kff.org/attachment/Supplemental-Tables-The-Uninsured-A-Primer-Key-Facts-about-Health-Insurance-and-the-Uninsured-Under-the-Affordable-Care-Act

Hull, G. & Pasquale, F. (2018). Toward a critical theory of corporate wellness. *BioSocieties13*(1), 190-212. Retrieved from: https://ssrn.com/abstract=3010313

Jones, D., Molitor, D., Reif, J. (2018, June). *What do workplace wellness programs do? Evidence from the Illinois workplace wellness study*. Cambridge, MA: National Bureau of Economic Research. Retrieved from https://www.nber.org/papers/w24229.pdf

Klein, J. (2003). *For all these rights: Business, labor, and the shaping of America's public-private welfare state*. Princeton, NJ: Princeton University Press.

Lakka, H.M., Laaksonen, D., Lakka, T., Niskanen, L., Kumpusalo, E., Tuomilehto, J., & Salonen, J. (2002). The metabolic syndrome and total and cardiovascular disease mortality in middle-aged men. *JAMA 288*(21), 2709-2716. doi:10.1001/jama.288.21.2709

Lamkin, M. (2013). Health care reform, wellness programs, and the erosion of informed consent. *101 Kentucky Law Journal 435*(2012-2013). Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2272244

Latonero, M. (2018). Big Data analytics and human rights. In M. Land & J. Aronson (Eds.) *New Technologies for Human Rights Law and Practice* (pp. 149-161). Cambridge: Cambridge University Press. https://doi.org/10.1017/9781316838952.007

Lupton, D. (2016). The diverse domains of quantified selves: Self-tracking modes and dataveillance. *Economy and Society 45*(1), 101-122. https://doi.org/10.1080/03085147.2016.1143726

Madden, M. (2017). *Privacy, security, and digital inequality: How technology experiences and resources vary by socioeconomic status, race, and ethnicity.* New York, NY: Data & Society. Retrieved from https://datasociety.net/pubs/prv/DataAndSociety_PrivacySecurityandDigitalInequality.pdf

Mattke, S., Liu, H., Caloyeras, J., Huang, C., Van Busum, K., Khodyadov, D., & Shier, V. (2013). *Workplace wellness programs study: Final report.* Santa Monica, CA: RAND Corporation. Retrieved from https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR254/RAND_RR254.pdf

O'Connor v. Uber Technologies, Inc. 82 F.Supp.3d 1133 (2015). Retrieved from https://scholar.google.com/scholar_case?case=6460059093768643370

Oravec, J. A. (2018). Intimate infiltrators: Ethical issues in the integration of self-tracking practices into workplace contexts. Presented at *International Association for Media and Communication Research Conference 2018*.

Pasquale, F. (2017). Epilogue: Professional cooperation and rivalry in the future of data-driven healthcare. *U of Maryland Legal Studies Research Paper No. 2017-32*. Retrieved from https://ssrn.com/abstract=3067560

Patient Protection and Affordable Care Act, 42 U.S.C. § 300gg-4(j)(3)(A) (2010).

Pearlman, S., Young, E., & Weinstein, A. (2017, October 13). The new wave of employee biometrics class actions. *LexisNexis Law360*. Retrieved from https://www.law360.com/cybersecurity-privacy/articles/972212/the-new-wave-of-employee-biometrics-class-actions

Ruckenstein, M. & Schüll, N. (2017). The datafication of health. *Annual Review of Anthropology 46*, 261-278. https://doi.org/10.1146/annurev-anthro-102116-041244

Slomovic, A. (2017). eHealth and privacy in U.S. employer wellness programs. In R. Leenes, N. Purtova, & S. Adams (Eds.), *Under Observation: The Interplay between eHealth and Surveillance* (pp. 31-58). Switzerland: Springer. doi:10.1007/978-3-319-48342-9 Retrieved from https://ssrn.com/abstract=2613452

Smith, G. (2016). Surveillance, data and embodiment: On the work of being watched. *Body & Society 22*(2). 108-139. doi:10.1177/1357034X15623622

Tankard, C. (2016). What the GDPR means for businesses. *Network Security 2016*(6), 5-8. https://doi.org/10.1016/S1353-4858(16)30056-3

Terry, N. (2012). Protecting patient privacy in the age of Big Data. *UMKC Law Review 81*(2). 385-415. Retrieved from https://heinonline.org/HOL/P?h=hein.journals/umkc81&i=397

Till, C. (2014). Exercise as labour: Quantified Self and the transformation of exercise into labour. *Societies 2014*(4), 446-462. doi:10.3390/soc4030446

Wachter, S. (2018). Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR. *Computer Law & Security Review 34*(3). 436-449. https://doi.org/10.1016/j.clsr.2018.02.002