Article

Surveillance Capitalism, Datafication, and Unwaged Labour: The Rise of Wearable Fitness Devices and Interactive Life Insurance

Constantine Gidaris

McMaster University, Canada
gidarisc@mcmaster.ca

Abstract

This paper examines the relationship between interactive life insurance companies and their policyholders and the way in which wearable fitness devices are deployed by these companies as data-generating surveillance technologies instead of personal health and fitness devices. Working within an expanded framework of “surveillance capitalism” (Zuboff 2015), I argue that while the notion of self-care generally associated with wearable fitness devices is underpinned by neoliberal constructs, the incentivization of interactive life insurance programs works to obscure the immense value placed on information capital. This paper briefly considers the legal loopholes involved in the harvesting of sensitive health and fitness information from consumer wearables and suggests that the push toward fitness trackers has little to do with any real concerns for the health and fitness of consumers and policyholders. Lastly, I consider different forms of unwaged labour in the relationship between policyholders and interactive life insurance programs. I contend that policyholders do not recognise the free and immaterial labour that goes into sustaining the data-based business model that interactive life insurance companies and social media platforms use and rely on for profit. In so doing, they relinquish power and control over the data they work to produce, only so that the information can be commodified and used against them.

Introduction

On September 19, 2018, Marianne Harrison, the CEO and President of John Hancock Life Insurance, the US division of Canada’s Manulife Financial Corporation, joined CNBC to explain the company’s exclusive shift toward providing data-driven life insurance policies, known more broadly as interactive life insurance. According to Harrison, John Hancock’s new Vitality Program, quite similar to Manulife’s Vitality Program, “is really about bringing technology based wellness...and marrying that with an insurance product” (CNBC 2018). In exchange for the data collected from consumer wearable fitness devices, policyholders earn Vitality Points through the John Hancock Vitality app, thus, participating in what the insurance provider deems as “everyday healthy activities” that range from exercise and healthy eating to meditation and good sleeping habits (John Hancock 2018). In addition to accumulating Vitality Points and up to fifteen per cent in savings on annual premiums, policyholders receive numerous discounts through retailers and e-commerce websites, including Walmart and Amazon, and discounts on an array of wearables such as Fitbit, Garmin, Polar, and Apple Watch (John Hancock 2018). The evolution of surveillance technologies under what Shoshana Zuboff calls “surveillance capitalism,” in which these and other technologies contribute to a new logic of information accumulation, conceal the ways in which vast amounts of data are produced and

consumed on an everyday basis (2015: 75). For interactive life insurance companies, these processes, including the collection, analysis, and selling of policyholder data, occur in ways and digital spaces that are commonly inaccessible by both policyholders and the general public. My intention within the scope of this paper is to build on Zuboff's claim that "information capitalism aims to predict and modify human behaviour as a means [of] produc[ing] revenue and market control" (2015: 75). I argue that by incentivizing interactive life insurance policies, companies like Manulife Financial Corporation exploit policyholder data by blurring and merging notions of everyday wellness with forms of self-tracking and top-down surveillance. By concealing the labour of the policyholder and the manipulation of their data behind notions of improved health and fitness, as well as discounts and savings on insurance premiums, interactive life insurance companies drive up their profits by capitalizing on the perpetual supply of data provided by the digitised bodies of their policyholders.

Wearables and the Digitisation of Self-Care

We might consider these technologies and those who use them as part of broader neoliberal models of consumption. In exchange for discounts and savings on insurance premiums, individuals offer up their data "for continuous, pre-emptive analysis, tracking, profiling, [and] targeting" (Graham 2011: 67). By contributing to this bottom-up yet top-down form of surveillance, individuals take on the neoliberal championing of selfhood and self-care (Lupton 2016: 52). This is not to suggest that self-care is implicated in some covert, neoliberal surveillance schema. Rather, it suggests that this technologically mediated form of self-care contributes to and reproduces existing social inequalities ingrained in the Canadian health care system. We know that income inequalities in Canada have a direct correlation and bearing on health inequalities. Individuals with higher incomes tend to experience better health results, whereas those with lower incomes tend to experience increased mortality rates and, more generally, worse health outcomes (Canadian Institute for Health Information 2016: 31). By advocating for a neoliberal understanding of self-care and self-responsibility, the notion of a responsible citizenry is reframed as one that engages in a digitised form of self-care, regardless of how the subsequent transmission of personal, medical, and health-related data are used by corporations and third party entities. In addition to using wearable fitness devices as digital tools of responsible self-care, individuals who secure interactive life insurance also secure their place in the socioeconomic hierarchy. They not only demonstrate their financial prowess as privileged individuals who can afford life insurance policies but they also demonstrate how time also functions as a barometer of socioeconomic status. In this championing of technologically mediated self-care, the digitised body emerges as the paradigm of what we might more accurately call neoliberal self-care. Here, the individual takes on the (pre-emptive) responsibility of their health and fitness through their connected wearable device. How their information is ultimately used, manipulated, or exploited by surveillance capitalism becomes a topic of less concern than that of their apparent individual health and fitness.

José van Dijck explains that surveillance differs from dataveillance—or "the monitoring of citizens on the basis of their online data"—on account that the former is used for specific monitoring purposes whereas the latter "entails the continuous tracking of (meta)data for unstated preset purposes" (2014: 205). As part of the digital economy, consumer wearable fitness devices offer associated apps, platforms, corporations, and third parties unobstructed access to sensitive medical and health-related data. Prior to the consumerization of wearables, access to such data was limited, by and large, to the medical community and legally safeguarded by doctor-patient confidentiality. While more traditional life insurance companies can access sensitive medical information from physicians, usually with the consent of policyholders through what is commonly referred to as a medical release form, gaining access to the sheer quantity of real-time digital data provided by wearable devices, mobile apps, and platforms is simply not feasible for traditional life insurance companies. The technology embedded in fitness trackers offers interactive life insurance companies a way to bypass the legalities and formalities involved in the retrieval of sensitive volumes of data. Beyond using sensors to measure different forms of exercise, the Fitbit Charge 2, for example, measures and records sleep quality through a process known as actigraphy, which means "translat[ing] wrist movements into sleep patterns" (Nield 2017). The Fitbit Charge 2 also uses optical sensors to measure heart rate by shining light on the user's skin to record their pulse, effectively illuminating the capillaries to

measure “the rate at which...blood is being pumped” (Nield 2017). Wearables are not only equipped with technology that measures and relays streams of data according to the physical movements of the body but they are also equipped with technology that is always “looking” inside the body. This non-invasive penetration of the human body, for the purpose of extracting sensitive data from within it, achieves what even medical wearables could not in the past: namely, to automate and delocalise the process of data collection and analysis while making it available for purchase and consumption.

Matthew R. Langley observes that sensitive medical and health-related information, collected and sold for profit, is not protected by law (2015: 1642). He remarks that, “[a]s the law currently stands, nothing is stopping health-app companies from selling this collected information to third parties” (2015: 1642). Although Langley’s legal analysis of wearables focuses on US federal law, much of it applies to Canada. As is evident from the Office of the Privacy Commissioner of Canada (OPC), the onus of privacy for owners of wearables falls squarely on the shoulders of individual consumers. While the OPC acknowledges that wearables collect and extract data about individuals and their everyday activities and that such data “can be processed, interpreted, aggregated, stored and shared with others” (Office of the Privacy Commissioner of Canada 2017; hereafter, OPC), the responsibility of data privacy is situated directly on the consumer. According to the OPC, the only viable recourses available to protect one’s data are to read privacy policies and terms of agreements prior to purchasing wearable devices, to choose strong privacy settings and passwords, and to shut off wearable devices as a means of limiting the amount of personal data that can be transmitted by them (OPC 2017). Wearables that were demarcated and strictly used as medical or health care devices in the past were governed by privacy standards set out by the Department of Health and the Federal Drug Administration (FDA) (Langley 2015: 1642). However, since consumer wearables are not prescribed as medical or health care devices in either the US or Canada, the data they transmit are not protected by any legal governing bodies. With the majority of wearable devices advertised as technologies that promote healthier living, they avoid being subjected to the same scrutiny as medically issued wearables. And while Europe has made some headway in protecting the privacy rights of individuals, with the introduction of the General Data Protection Regulation on May 25, 2018, the US and Canada have yet to follow suit.

The increasing global demand for connected wearable devices, estimated to reach nearly one billion units by 2021 (Statista 2017), demonstrates how popular these devices have become. The move toward wearable fitness trackers constitutes one that can be partly explained by what Deborah Lupton calls a “techno-utopia” (2016: 59). As Lupton shows, these digital devices “extend the capacities of the body by supplying data that can then be used to display the body’s limits and capabilities,” positioning these devices as innovative and progressive ways of promoting health and happiness (2016: 59). In this view, users of wearable fitness devices also surrender their data in exchange for achieving a degree of techno-utopia. Their vision of a perfect, healthy body is one that becomes digitally conditioned by and inseparable from the data that are supplied to them through their wearable devices. This techno-utopian rationale, however, is troubled by the fact that many wearable users abandon their devices after a short period of time. As Dan Ledger and Daniel McCaffrey explain, “most of these devices fail to drive long-term sustained engagement for a majority of users” (Ledger and McCaffrey 2014). Their research reveals that while one third of wearable consumers in the US stop using their devices within six months, more than half of them no longer use them at all (Ledger and McCaffrey 2014). For Ledger and McCaffrey, long-term consumer engagement is a matter of functionality, which, as they conclude, relies on three key behaviour related factors: habit formation, social motivation, and goal reinforcement (Ledger and McCaffrey 2014). What their research does not take into account is that long-term user engagement with wearables is a far more pressing issue for those engaged in surveillance capitalism. In the market sphere, the relevance of wearable functionality for long-term user engagement is premised on the capacity to sustain it for the sole purpose of accumulating information capital. Whether we consider design, functionality, or behaviour-related factors, the underlying function of wearable fitness devices is to generate data that can turn a profit. Without serving this basic purpose, wearable fitness devices, along with their mobile apps and platforms, are rendered rather useless for companies.

Another way in which surveillance capitalism ensures the sustainability of its flow of information capital is to augment long-term user engagement through incentivization. In Canada, the incentivization of wearable devices is particularly evident through Manulife's Vitality Program, which is affiliated with a number of rewards partners, including Hotels.com, Garmin, Amazon, ExamOne, and Goodlife Fitness (Manulife 2018). With rewards partners offering financial incentives, accumulated and earned through Vitality Points and one's Vitality Rewards Status, policyholders are given more reason to not only commit to their wearable fitness devices in the long-term but also to keep their wearables on and functioning at all times. For interactive life insurance companies like Manulife, this has largely to do with the fact that activity and inactivity are both imperative in the process of datafying their policyholders. Linking devices like Fitbit, Garmin, or Apple Watch to the Manulife Vitality mobile app or online portal enables the transmission of data obtained from both physical activity and inactivity, including dietary choices and sleeping patterns. The data that are subsequently shared, bought, and sold in the digital data market are used, in part, to commercially target individuals with specific retail products or services. As Christian Fuchs observes, "precise user data and aggregated data can be sold to advertising clients who, armed with information about potential consumption choices, provide users with personalized advertising that targets them in...everyday situations" (2011: 291). For instance, tracking an individual's sleep patterns "could lead to a timely brochure from a mattress company" (Langley 2015: 1646).

The information furnished by connected wearables not only provides companies with the power to target individuals with advertisements, products, and services but it also carries the potential of being punitively deployed. By giving Manulife Vitality permission to share their data, new policyholders begin earning and accumulating points toward a higher Vitality status. As they begin to collect Vitality Points, they increase their Vitality status, moving from "bronze, to silver, to gold and, ultimately, platinum" (Manulife 2018). The higher one's Vitality status becomes, the more eligible they are for rewards that include retail discounts and savings on insurance premiums (Manulife 2018). Yet, despite all this, interactive life insurance companies can use policyholder data in ways that are detrimental to the policyholder. For insurance providers, physical activity is only recognised as such when it generates data through a technological medium, neglecting the importance of non-physical forms of exercise and mental health. Moreover, it raises important questions about how datafied activity and inactivity can affect policyholders. If physically active policyholders can earn points, rewards, and discounts for their progress, could less active policyholders be held accountable for their inactivity in other ways? As Langley inquires, might a "relatively inactive week [...] potentially cause an individual to be deemed a 'health risk' in the eyes of his or her insurance provider?" (2015: 1647). Will the constant collection and monitoring of an individual's data, authorise interactive insurance providers to increase premiums based, for example, on a combination of physical inactivity, poor dietary choices, and poor sleeping habits? Could this data be used by interactive life insurance companies to establish a breach of contract, when, perhaps, an individual's health and fitness data can be connected, however loosely, to newly developed medical conditions or diseases?

The Labour of Coverage

In all of this, what is often forgotten is the labour of the interactive life insurance policyholder. As Lupton suggests, we can partly think of this in terms of a "shift from commodifying workers' bodily labour to profiting from information collected on people's behaviours, habits and preferences" (2016: 48). This type of labour contributes to what Lupton and others refer to as "prosumption," a term that "denotes the ways in which people interacting with online technologies and other digital devices simultaneously consume and create digital content" (2016: 48). Fuchs espouses the idea that we think of the prosumer as a more contemporary version of Karl Marx's proletariat, "who directly or indirectly produce[s] surplus value and [is] thereby exploited by capital" (2011: 297), or, in this case, information capital. If we consider the data-driven physical activity of policyholders as free labour in the digital economy, interactive life insurance policyholders emerge as typical prosumers. That is, the distinction between them as producers and consumers is blurred, as the surplus value they produce in the form of data are used and consumed by them, by insurance companies, and by a host of other third parties, without remuneration. On one hand, interactive life insurance providers benefit from the incentivised free data provided by the labour of their policyholders.

On the other hand, they benefit from the insurance premiums that policyholders pay for their coverage. As prosumers, policyholders are paradoxically exploited for the streams of free data they produce through the insurance premiums they pay to their insurance providers.

Fuchs emphasises a critical point in the exploitation of surplus value, particularly when we apply it to interactive life insurance companies. He argues that because “surplus value generating labour is an emergent property of capitalist production,” the withdrawal of this form of labour would collapse without the user-generated production and accumulation of information capital (2011: 298). Fuchs suggests, and rather astutely, that if prosumers stopped using social media platforms—in other words, if they ceased producing user-generated content—“the number of users would drop, advertisers would stop investments because no objects for their advertising messages and therefore no potential customers for their products could be found, the profits of new media corporations would drop, and they would go bankrupt” (2011: 298). We can likewise imagine a similar scenario for interactive life insurance companies. If policyholders stop generating data through their connected wearable devices, interactive life insurance companies would likely cease to exist. Similar to YouTube, Twitter, and Instagram, the business model of interactive life insurance companies is heavily dependent on user-generated content. With prosumption, the user of online technologies emerges as the product or the commodity (Lupton 2016: 49; Fuchs 2011: 298). For this reason, “[t]he value of the data that prosumption produces explains why so many services such as social media platforms and apps are offered for free” (2016: 49), including those offered by wearable fitness devices and interactive life insurance companies.

Another iteration of labour we might consider in the relationship between the interactive life insurance provider and the policyholder is that of immaterial labour. The concept of immaterial labour, as defined by Maurizio Lazzarato, consists of “labour that produces the informational and cultural content of the commodity [and] refers to *two different aspects of labor*” (1996: 133). The first, in terms of the informational component of the commodity, is that it reflects the changes in the workplace, “where the skills involved in direct labor are increasingly skills involving cybernetics and computer control” (1996: 133). The second is in regard to the cultural component of the commodity and is that “immaterial labor involves a series of activities that are not normally recognized as ‘work’” (1996: 133). In this sense, we can view the delocalised, digital labour of the policyholder according to the informational content they provide as digital data. We can also view the delocalised, physical labour according to the cultural content of the commodity they provide, labour that revolves around the physical activities of the policyholder, which are not traditionally regarded as work.

In considering what Joyce Goggin calls “playbour” in the video game industry, Goggin argues that previously demarcated boundaries of work and non-work are blurred when employees are immersed in a “culture of fun” that encourages them to “see work as an extension of their own volition” (2011: 358). Although policyholders are not considered employees in any real sense, particularly because they are unwaged workers, their unwaged labour qualifies as a sort of playbour since what constitutes play rather than work hinges not only on the idea of wages but also on the idea of agency (2011: 359). If playbour also relies on the question of agency, then the choice policyholders make to participate in interactive life insurance programs, at least for the time being, remains a voluntary one. Their labour, or that which their bodies produce in the form of data, can be seen as part of a fun online game that incentivises the player through a system of rewards and punishments. Like conventional video games, which employ the tactic of in-game mechanisms to reward and discipline players (2011: 363), the gameplay of policyholders operates along a similar trajectory of reward and punishment. That is, those who play the game of interactive life insurance well, by amassing as many Vitality Points as they can and, thereby, increasing their Vitality Rewards Status, are rewarded through a number of discounts and premiums. However, those who fail to maximise their gameplay by failing to maximise their data output are not rewarded with the same level of discounts and premiums. The game embedded in interactive life insurance programs makes the notion of fun contingent on the policyholder’s capitulation of sensitive data to the insurance provider and anyone willing to pay for it.

Conclusion

As Lupton writes, “[t]he nexus of human bodies, digital devices, sensor-embedded spaces and data offers some intriguing possibilities for thinking through the contemporary experience of the digitised human” (2016: 56). This is especially true for how we think about the relationship between the physical and digitised body of the interactive life insurance policyholder. By viewing the physical body as a site of quantifiable information that can be used by the policyholder and the insurance company to manage, control, and monitor health and fitness levels, the body becomes nothing more than a data-generating machine. With the evolution of the body as machine metaphor, from the portrayal of the body at the time of the Industrial Revolution “as an engine, with pistons and pumps,” to the portrayal of the body in the Information Age as a “digital information system,” there has been a shift in the ways we have come to know, treat, and understand the human body, from the haptic to the visual (2016: 58). Lupton explains that “[w]here once people relied upon the sensations they felt in their bodies and reported to their physicians” (2016: 59), medical technologies have altered experience and ways in which bodies are treated by generating data that are “privileged as more ‘objective’ than the signs offered by the ‘real’, fleshly body and the patients’ own accounts of their bodies” (2016: 59). While perhaps understating the value of self-haptic knowledges and the role that physicians play in medical diagnoses, wearable fitness devices digitise the body with a surveillance capitalist and automated extremism. Unlike medical technologies, which look inside the body for the purpose of assisting in its diagnosis, connected wearables are constantly peering inside the body as a way of commoditizing and commodifying the information it produces.

The torrents of data that are supplied to interactive life insurance companies have less to do with improving the health and fitness of their policyholders and more to do with sourcing the data in the most profitable of ways. Whether individuals who use wearable fitness devices are in fact “healthier” or “more fit” than those who do not is not an argument this paper takes up. Indeed, there may very well be health and fitness benefits to using such devices. What becomes rather apparent, however, is that wearable fitness devices do not operate in social or financial isolation, free from the clutches of surveillance capitalism. The data harvested from these devices becomes part of a larger “surveillant assemblage,” which, as Kevin D. Haggerty and Richard V. Ericson explain, “operates by abstracting human bodies from their territorial settings and separating them into a series of discrete [data] flows” (2000: 606). For interactive life insurance companies, the only significant value the human body possesses is in its capacity to be abstracted. By abstracting human bodies into data flows that can be exchanged, purchased, and sold in the digital economy, these companies look to the body as a digital site, one whose value is predicated entirely on its capacity to yield profitable information.

References

- Canadian Institute for Health Information. 2016. Trends in Income-Related Health Inequalities in Canada. *Technical Report*, 1-291. <https://bit.ly/2zrZO52> [accessed November 18, 2018].
- CNBC Television. 2018. John Hancock to Only Provide Data-Driven Life Insurance. *YouTube*, September 19. https://www.youtube.com/watch?v=3kl0t1rD_A4 [accessed November 1, 2018].
- Fuchs, Christian. 2011. Web 2.0, Prosumption, and Surveillance. *Surveillance & Society* 8 (3): 288-309.
- Goggin, Joyce. 2011. Playbour, Farming and Leisure. Ephemera: Theory and Politics. *Organization* 11 (4): 357-368.
- Graham, Stephen. 2011. *Cities Under Siege: The New Military Urbanism*. London: Verso.
- Haggerty, Kevin D., and Richard V. Ericson. 2000. The Surveillant Assemblage. *British Journal of Sociology* 51 (4): 605-622.
- John Hancock. 2018. *John Hancock Life Insurance*. <https://bit.ly/2Or5FQN> [accessed November 1, 2018].
- Langley, Matthew R. 2015. Hide Your Health: Addressing the New Privacy Problem of Consumer Wearables. *The Georgetown Law Journal* 103: 1641-1659.
- Lazzarato, Maurizio. 1996. Immaterial Labour. In *Radical Thought in Italy: A Potential Politics*, edited by Paolo Virno and Michael Hardt, 132-146. Minnesota: University of Minnesota Press.
- Ledger, Dan, and Daniel McCaffrey. 2014. Inside Wearables: How the Science of Human Behavior Change Offers the Secret to Long-Term Engagement. *Medium*, January. <https://bit.ly/2SUzIjj> [accessed November 2, 2018].
- Lupton, Deborah. 2016. *The Quantified Self: A Sociology of Self-Tracking*. Cambridge, UK: Polity.
- Manulife. 2018. *Manulife Vitality*. <https://www.manulife.ca/for-you/insurance/vitality.html> [accessed November 2, 2018].

- Nield, David. 2017. How it Works: We Explain How Your Fitness Tracker Measures Your Daily Steps: From the Sensors to the Algorithms, This is How Your Fitness Tracker Works its Magic. *Wearable*, December 31. <https://bit.ly/2k2U11A> [accessed November 2, 2018].
- Office of the Privacy Commissioner of Canada. 2017. *Wearable Devices and Your Privacy*. <https://bit.ly/2PPtQcA> [accessed November 2, 2018].
- Statista. 2017. Number of Connected Wearable Devices Worldwide from 2016 to 2021 (in millions). *Statista: The Statistics Portal*. <https://bit.ly/2jjuH33> [accessed November 2, 2018].
- Van Dijck, José. 2014. Datafication, Dataism and Dataveillance: Big Data Between Scientific Paradigm and Ideology. *Surveillance & Society* 12 (2): 197-208.
- Zuboff, Shoshana. 2015. Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology* 30: 75-89.