The Wellness Cure for the Workplace: Human Capital Law as a Lens for Considering Personal Health Data Beyond Privacy

Margot Parmenter*

* © 2017 Margot Parmenter. Margot Parmenter is a Research Fellow at the Institute of Law, Politics and Development at the Scuola Superiore Sant'Anna in Pisa, Italy. She received her Bachelor of Civil Law from the University of Oxford (2016) and also holds degrees from Pepperdine University School of Law (J.D., *summa cum laude*, 2013) and the University of Chicago (A.B., History, 2010).

"The formula for happiness . . . remains a trade secret."

—Takashi Mochizuki[1]

"Unlike money or equipment, this type of capital cannot conceptually be separated from the individual who owns it. It's intrinsically part of him. And by extension, someone's human capital cannot be owned by anyone else since that would be slavery. Therefore, who exactly ought to have the responsibility of investing in it or the enjoyment of its benefits?"

—Peter Fleming, discussing human capital[2]

I. INTRODUCTION

There is a revolution happening in the workplace. Slowly but surely, Big Data is infiltrating traditional employment relationship structures, fundamentally changing both industry and society. Although this "datafication" of the workplace is changing not only how we work but also how we live in ways that remain nascent, we are, for the most part, blind to its occurrence and uncertain about its import. In the legal scholarship, this blindness has taken the shape of a perspectival narrowness: much of the research examining the ways in which Big Data is altering the employment relationship is framed from a privacy perspective that harbors particular ontological and sociocultural assumptions that shape the relevant reasons for concern—and, in turn, the proffered solutions.[3]

---

1. Takashi Mochizuki, *Hitachi Unlocks the Key to Happiness*, WALL ST. J. (Feb. 9, 2015, 5:18 PM), http://blogs.wsj.com/japanrealtime/2015/02/09/hitachi-unlocks-the-key-to-happiness/ (referring to Hitachi's wearable sensor technology, which is designed to analyze and enhance workplace productivity by charting and subsequently designing for employee happiness).

2. Peter Fleming, *What Is Human Capital?*, AEON (May 10, 2017, 10:29 PM), http://aeon.co/essays/how-the-cold-war-led-the-cia-to-promote-human-capital-theory.

3. *See, e.g.*, Robert Sprague, *Welcome to the Machine: Privacy and Workplace Implications of Predictive Analytics*, 21 RICH. J.L. & TECH., no. 2, 2015, at 1, http://jolt.richmond.edu/jolt-archive/v21i4/article13.pdf; Frank Pasquale & Tara Adams Ragone, *Protecting Health Privacy in an Era of Big Data Processing and Cloud Computing*, 17 STAN. TECH. L. REV. 595, 595, 597 (2014).

The scholarship is also inevitably hostage to historical trajectory; much of the present discussion of personal data in the workplace is undertaken through the lens of health. Outside of more traditional forms of employee tracking, which have raised privacy concerns throughout modern history,[4] the rise of mobile Health applications (often referred to as "mHealth"), employee wellness programs, and the quantified self movement together constitute one of, if not the most, significant intersections of Big Data and the workplace. Because of this historical reality, the current conversation about the datafication of the workplace often revolves around the question of employer access to and use of employee health or health-adjacent information. While there is recognition in the popular literature that the workplace implications of the Big Data revolution extend beyond the realm of privacy,[5] no other empirical example is as high-profile as that of the workplace-health data crossover. By now, the employer-funded or employer-accessed Fitbit is almost a trope in the field—just a gesture to it and we all know what we are talking about: Does this data count as protected "personal" or "sensitive" data? Who owns it? Should employers have unlimited access? Can they share it? Can they use it to make employment decisions?

This Article departs from that discursive trend, with the twin aims of highlighting some of its limitations and drawing attention to the progressive breadth and depth of the workplace Big Data revolution, which must be met with a variety of analytic frameworks in order to comprehensively map its import and desirability. To do so, I focus herein on a particular sort of data that is distinct from and yet related to the health-adjacent data collected by personal fitness devices.[6] I refer to this

---

4. *See* Corey A. Ciocchetti, *The Eavesdropping Employer: A Twenty-First Century Framework for Employee Monitoring*, 48 AM. BUS. L.J. 285, 285 (2011).

5. *See, e.g.*, Josh Bersin, *The Geeks Arrive in HR: People Analytics Is Here*, FORBES (Feb. 1, 2015, 6:12 PM), http://www.forbes.com/sites/joshbersin/2015/02/01/geeks-arrive-in-hr-people-analytics-is-here/2/#24baca932902; Olga Khazan, *Thinking Outside the Cube*, ATLANTIC (Sept. 2015), http://www.theatlantic.com/magazine/archive/2015/09/thinking-outside-the-cube/399374/; Steven Melendez, *The Office Is Watching You*, FAST COMPANY (May 22, 2015), http://www.fastcompany.com/3046133/the-future-of-workplace-surveillance.

6. There is a burgeoning literature addressing the borderline "sensitivity" of this kind of data, which typically falls beyond the bounds of protected legal data categories, thus failing to attract legal protection as health data despite its capacity for revealing granular personal detail. *See, e.g.*, Michelle M. Christovich, *Why Should We Care What Fitbit Shares?: A Proposed Statutory Solution To Protect Sensitive Personal Fitness Information*, 38 HASTINGS COMM. & ENT. L.J. 91, 92 (2016) (referring to the "various types of sensitive information collected by [personal activity monitors]" as "personal fitness information" and enumerating it—"user's heart rate, number of steps taken, activity levels, sleep quality and duration, and calories burned").

type of data as "productivity data" and attempt to sketch its relationship to the other varieties of data at issue in the health and health-adjacent data ecosystem. After mapping productivity data onto the existing landscape, this Article proceeds to consider the way in which this type of data raises different kinds of concerns and falls under a different legal and social paradigm than the one currently dominating the scholarly analysis. To highlight the characteristics of this alternative paradigm, this Article introduces the lens of human capital law, that bundle of regulatory and contractual structures relating to the brokerage of ownership in the knowledge economy. Finally, this Article offers several suggestions regarding the insights that deployment of this lens can reveal for both the treatment of productivity data and the datafication of employment at large.

This Article proceeds in four Parts. Part II outlines the current contours of the personal health data privacy debate as they relate to the workplace, establishing a rubric of the various types of data that arise in the literature. Part III introduces the concept of productivity data and situates it within the health-data-in-the-workplace ecosystem, explaining the ways in which this kind of data is both distinct from and related to the other sorts of data at issue in the field. Part IV explicates the framework of human capital law, tracing the ways in which applying this legal framework to the datafication of the employment relationship yields a lacuna in the existing treatment of the issue, bringing into relief concerns different from those currently dominating the conversation. Part V offers three lessons from human capital law about personal health and health-adjacent data in the workplace, which will strengthen future attempts to meet the challenges of Big Data's workplace revolution.

II. A WEALTH OF INFORMATION: HEALTH, WELLNESS & THE SELF AT WORK

The current thrust of the literature relating to health and health-adjacent data in the workplace is animated by two cultural developments: (1) the explosion of the market for personal wearable fitness devices,[7] and (2) the trend by which corporate wellness programs capitalize on

7. *See* Ariana Eunjung Cha, *The Human Upgrade: The Revolution Will Be Digitized*, WASH. POST (May 9, 2015), http://www.washingtonpost.com/sf/national/2015/05/09/the-revolution-will-be-digitized/?utm_term=.5951d66455c4; *see also* Ariana Eunjung Cha, *The Problems with the Explosion in Fitness Tracking*, WELL & GOOD (May 11, 2015, 1:24 PM), http://www.stuff.co.nz/life-style/well-good/teach-me/68435451/the-problems-with-the-explosion-in-fitness-tracking.

such devices to nudge increasingly sedentary knowledge-based workforces toward healthy lifestyle choices in order to decrease insurance costs.[8] In the United States, the occurrence of these two events against the existing legal backdrop has generated a somewhat paradoxical, and perhaps untenable, situation. Although this wellness data is often treated by employers as health-type data, and sometimes even used to support decisions that directly affect health circumstances (perhaps conditioning payment of health-care premiums[9]), it does not fall within the purview of any existing privacy law.[10] This means that workers are now generating and sharing a wealth of health-related information that is not subject to any privacy or confidentiality protections. Indeed, because much of this data is not subject to any controls at all, it can be bought, sold, mined, processed, used, and reused in innumerable and unexpected ways, giving rise, along the way, to a variety of unanticipated and unsavory practices.[11] This technological outpacing of the regulatory mechanisms, along with employer motivation to deploy the information toward actual health-care-related outcomes, has infused the scholarly discussion[12] of the issue with a certain aim: closing the regulatory gap by designing and implementing privacy protections for this data that are commensurate with the ways it is being used—that are,

---

8. This second development is localized to the United States, where employer-provided insurance is the sociopolitical norm. Despite this localization, its influence on the contours of the scholarship in the field is noticeable. *See, e.g.*, Elizabeth A. Brown, *The Fitbit Faultline: Two Proposals To Protect Health and Fitness Data at Work*, 16 YALE J. HEALTH POL'Y L. & ETHICS 1, 13-15 (2016); Christovich, *supra* note 6, at 102-03, 108-09; Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 85 (2014).

9. *See* Christovich, *supra* note 6, at 102-04; *see also* Lauren Weber, *Wellness Programs Get a Health Check*, WSJ (Oct. 10, 2014), http://www.wsj.com/articles/wellness-programs-get-a-health-check-1412725776; PWC, FUTURE OF WORK: RESHAPING THE WORKPLACE 9, 11-12, 14-15 (2014), http://www.pwc.com/gx/en/services/people-organisation/workforce-of-the-future/workforce-of-the-future-the-competing-forces-shaping-2030-pwc.pdf.

10. *See* Nicolas Terry, *Protecting Patient Privacy in the Age of Big Data*, 81 U. MO.-KANSAS CITY L. REV. 385, 385-86 (2012) (recognizing that the modern "medical self" exists "outside of the traditional (and HIPAA/HITECH-regulated) health domain") (internal citations omitted).

11. Perhaps the most famous and oft-referenced example of this is the wellness program vendor Castlight Healthcare's use of data to predict employee pregnancy. *See* Ifeoma Ajunwa et al., *Health and Big Data: An Ethical Framework for Health Information Collection by Corporate Wellness Programs*, 44 J.L. MED. & ETHICS 474, 475 (2016); *see also* Matt Payton, *Employers Can Now Use Big Data To Find Out if You're Pregnant*, INDEPENDENT (Feb. 18, 2016, 6:49 PM), http://www.independent.co.uk/news/business/news/employers-can-now-use-big-data-to-find-out-if-youre-pregnant-a6881741.html.

12. *See, e.g.*, Christovich, *supra* note 6, at 92-93; *see also* Jerry Kang et al., *Self-Surveillance Privacy*, 97 IOWA L. REV. 809, 823 (2012).

in essence, health-data-like. The central distinction in the literature, then, is that between true health data—covered by existing federal law—and health-adjacent data, most typically the kind produced by wearable fitness devices.[13]

An added layer of complexity derives from the multipurpose nature of the wearable devices themselves, which, though capable of exploitation toward employer ends, are primarily marketed directly to consumers as tools for self-improvement in the context of what has been labelled the "quantified self" movement.[14] Indeed, employer access to, and use of, wellness data occupies only a small segment of a much larger sociocultural trend toward self-monitoring through the use of "smart," web-connected devices.[15] The existing legal literature is sensitive to this but nevertheless tends to treat even the broader movement, which encompasses the collection of data that have traditionally fallen outside of the confidential-data conceptual space,[16] through a privacy lens.[17] This is, perhaps, unsurprising, considering that all of these types of data come into being, empirically speaking, entangled with one another, generated by the same device as part of a suite of self-monitoring services.

As a final layer, the ascendance of data mining and analytics has given rise, within this ecosystem, to a sort of information that has only recently begun to hover in the same space as the raw data collected by wearable devices or medical tests specifically because analytic advances now enable such data to provide new and revealing insights about individuals. Borrowing from Frank Pasquale and Tara Adams Ragone, I refer to this type of data as "medical reputation" information[18] and attempt to trace the ways in which this final layer of seemingly

---

13. *See infra* Sections II.A-B.

14. Dominik Leibenger et al., *Privacy Challenges in the Quantified Self Movement—An EU Perspective*, 4 PROC. ON PRIVACY ENHANCING TECHNOLOGIES 315, 315 (2016).

15. The evolution of the "Internet of Things" involves monitoring a variety of self-extensions and environments. *See generally* Peppet, *supra* note 8.

16. Consider, e.g., mobility or location data—wearable devices and sensors can track location using GPS, a technological capability that raises privacy considerations but not necessarily health-infused ones. Such data can throw off privacy concerns (particularly in the context of long-term surveillance) but is not typically considered sensitive or confidential in itself. Issues surrounding it also remain unsettled within the U.S. legal system, particularly in light of the Supreme Court's narrowly grounded decision in *United States v. Jones*, 565 U.S. 400 (2012).

17. *See* Nicolas Terry, *Big Data Proxies and Health Privacy Exceptionalism*, 24 HEALTH MATRIX 65, 97-103 (2014) (framing the intersection of health law and big data as a privacy crisis, and stating that "big data challenges the core tenets of health privacy and its regulation") (internal citations omitted).

18. Pasquale & Ragone, *supra* note 3, at 629.

innocuous data colors each of the other types, casting confusion and ambivalence onto the discourse about how to define and treat health-type data in the workplace.

Thus, in my map of the current health-data conceptual sphere, there are three types of data: health data, self-quantification data, and medical reputation data. I enumerate the qualities and scholarly treatment of each in turn.

A. Health Data: The Paradigmatic Case

In the modern health and health-adjacent data privacy debate, traditional health data is the only thing about which we are sure. It has a settled social meaning and garners legal protection as a central case. Utilizing Helen Nissenbaum's language of context,[19] the central case involves data that is (1) produced within the channels of the health-care delivery system, (2) by health-care professionals interacting with individuals as patients, and (3) designed to be deployed within the confines of the system toward the optimization of care. In the United States, such data falls cleanly within the bounds of the Health Insurance Portability and Accountability Act (HIPAA).[20] HIPAA ensures the privacy of "personally identifiable health information" being held by "covered entities"[21] such as health-care providers, health plans, and health-care clearinghouses—along with any related business associates who manage protected information—via the establishment of certain confidentiality and security duties that such entities are required to uphold.[22] HIPAA, however, is confined to this very specific social context, applying only to "protected health information" (PHI), which is defined as "information relating to an individual's physical or mental health, health care service, or health care service payment that

---

19. Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119 (2004) (positing the notion of "contextual integrity" as a mode for understanding and instituting privacy).

20. *See* Latena Hazard, *Is Your Health Data Really Private? The Need To Update HIPAA Regulations To Incorporate Third-Party and Non-Covered Entities*, 25 CATH. U. J.L. & TECH. 447, 449 (2017) (quoting JOCELYN SAMUELS & KAREN B. DESALVO, U.S. DEP'T OF HEALTH & HUM. SERVS., EXAMINING OVERSIGHT OF THE PRIVACY & SECURITY OF HEALTH DATA COLLECTED BY ENTITIES NOT REGULATED BY HIPAA 13-14 (2016), http://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf).

21. *See* SAMUELS & DESALVO, *supra* note 20, at 11-12.

22. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), P.L. No. 104-191, 110 Stat. 1938 (1996); *see also* Heather Patterson, *Contextual Expectations of Privacy in Self-Generated Health Information Flows* 17-18 (Mar. 30, 2013) (working paper), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2242144.

[(1)] individually identifies that patient, and . . . [(2)] is created or received by a health care provider, health plan, employer, or health care clearinghouse."[23]

As is evident here, the statute defines this type of data by drawing directly from the context of its production—what qualifies it for protection is not some inherent characteristic of the raw data itself, but rather the social context in which it is generated. The fact that the delimitation of context is not constant—that social meanings and mores can change over time—is exactly the sort of reality that underlies the current disruption in the field, reshaping the ecosystem and riddling the literature with confusion. After all, the fact that the same bit of information—say, an individual's height or weight—will attract privacy protection if recorded in a doctor's office but not if done so at, for instance, a commercial gym, seems somewhat counterintuitive. Nevertheless, it draws our attention to an important aspect of the health and health-adjacent data ecosystem, which is that the social meaning of data is a key—but often overlooked—driver behind both our cultural, political, and legal responses to it and our regulatory suggestions about it. It is my aim in the later parts of this Article to demonstrate that, because of certain historical and circumstantial developments, the legal scholarship in this arena has misread the social meaning of some of the data in this space, with the result of an anemic analytic perspective.

That the health-care context and the physician-patient relationship is the key defining feature of the central data case on our map—health data—is reinforced by the way in which the U.S. regulatory regime attempts to parse the proliferation of data accompanying the expansion of mobile technology and self-monitoring capacities. The Food and Drug Administration (FDA), the federal agency charged with controlling pharmaceuticals and medical devices (among other things), has chosen to direct its regulatory oversight only to those applications that effectively transform a mobile platform into a medical device.[24] This would exclude "general health and wellness" apps used solely to "log, track, evaluate, or make decisions or suggestions related to developing or maintaining

---

23. *See* Patterson, *supra* note 22, at 16; *see also* Brown, *supra* note 8, at 25-27.

24. *See* FOOD & DRUG ADMIN., MOBILE MEDICAL APPLICATIONS: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF (Feb. 9, 2015) [hereinafter MOBILE MEDICAL APPLICATIONS], http://www.fda.gov/downloads/MedicalDevices/.../UCM263366.pdf; *see also* FOOD & DRUG ADMIN., GENERAL WELLNESS: POLICY FOR LOW RISK DEVICES GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF (July 29, 2016), http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm429674.pdf.

general health and wellness," where such tracking is not intended to cure, treat, seek treatment and/or mitigation for, or diagnose any specific disease, disorder, patient state, or identifiable health condition.[25] The distinction between a regulated and an unregulated app employed here largely references the clinical health-care context. Where an app is designed to enhance the clinical environment—by, for example, extending control of patient monitoring tools to a mobile platform (as when bedside monitors or blood pressure cuffs can be controlled remotely within the clinical environment), or assisting health-care professionals in providing patient-specific treatment recommendations—it falls within regulated territory.[26] Where, on the other hand, an app is designed to be used by the individual outside of this context, for self-management or tracking, it falls outside the regulated space.[27] The latter type of app is, of course, the kind most commonly deployed in the self-quantification movement. The data associated with that movement is the second type on our map.

B. Health-Adjacent Data: By Me, for Me—Self-Quantification & Monitoring

Moving beyond the central case takes us to the type of data that is currently at the crux of the conversation—data produced via the assistance of personal wearable monitors like Fitbit, Jawbone, and Apple Watch. This type of data encompasses a variety of different sorts of measurements, but it is most typically treated by the literature as a coherent class unto itself, likely because all such measurements share the defining features of being (1) about the self and (2) consciously gathered at the behest of the self.[28] In other words, this sort of data—much like

---

25. Patterson, *supra* note 22, at 19-20 (quoting FOOD & DRUG ADMIN., DRAFT GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF, MOBILE MEDICAL APPLICATIONS 11 (July 21, 2011) (updated by MOBILE MEDICAL APPLICATIONS, *supra* note 24)).

26. *See* 21 U.S.C. § 321(h)(2) (2012); *see also* MOBILE MEDICAL APPLICATIONS, *supra* note 24, at 14-15 (providing examples of mobile apps that are the focus of FDA regulatory oversight and those for which the FDA does not intend to enforce requirements); Stephen McInerney, *Can You Diagnose Me Now? A Proposal To Modify the FDA's Regulation of Smartphone Mobile Health Applications with a Pre-Market Notification and Application Database Program,* 48 U. MICH. J.L. REFORM 1073, 1081-82 (2015).

27. *See* MOBILE MEDICAL APPLICATIONS, *supra* note 24, at 14-15, 23-25; *see also* Lindsay Kobayashi, *How Does the FDA Regulate Mobile Medical Apps?*, PLOS: PUB. HEALTH PERSP. BLOG (Mar. 2, 2015), http://blogs.plos.org/publichealth/2015/03/02/fda-apps/.

28. *See, e.g.*, Helen Nissenbaum & Heather Patterson, *Biosensing in Context: Health Privacy in a Connected World*, *in* QUANTIFIED: BIOSENSING TECHNOLOGIES IN EVERYDAY LIFE 79 (Dawn Nafus ed., 2016).

the traditional health data examined in the previous Section—is distinguished by the mode of production and not necessarily by the features of the raw bits of data themselves.[29]

Scott Peppet provides a concise but comprehensive overview of the type of information collected by such devices: steps taken each day, distance walked, calories burned, minutes asleep, quality of sleep, heart rate, perspiration, skin temperature, breathing patterns, running or sporting technique, and posture.[30] Heather Patterson notes additional data dimensions enabled by user interaction—consumers inputting certain data into the tracker—and other features, asserting that self-tracking tools "encompass a broad range of information types, including detailed longitudinal portraits of individuals' states, behaviors, signals of clinical conditions, physiological biomarkers, personal goals, and even real-time geospatial locations."[31] Although not yet ubiquitous, the use of wearable personal fitness devices has been on the rise over the past several years, a trend that is predicted to continue.[32] In 2015, the wearables market exceeded $2 billion, and it is expected to hit over $4 billion in 2017.[33] Approximately 50 million wearable devices were shipped in 2015, with over 125 million units expected to ship in 2019.[34] Additionally, one in every six U.S. consumers currently owns and uses some version of wearable tech.[35]

This rapid expansion, which has taken place within just the past ten years,[36] is notable not only in itself but also in what it reveals about the context of self-quantification data. The explosion in wearable self-

---

29. *See id.*

30. Peppet, *supra* note 8, at 101-02.

31. Patterson, *supra* note 22, at 6.

32. Bernard Marr, *15 Noteworthy Facts About Wearables in 2016*, FORBES TECH (Mar. 18, 2016, 2:16 AM), http://www.forbes.com/sites/bernardmarr/2016/03/18/15-mind-boggling-facts-about-wearables-in-2016/#39c571c52732. Note that the wearables market includes a variety of sensor-bearing devices and is somewhat broader than the fitness and health tracker market.

33. *Id.*

34. *Id.*

35. *See* Christovich, *supra* note 6, at 93-94. A different study indicates that the number of wearable owners is closer to one in five. *See* Jonah Comstock, *PwC: 1 in 5 Americans Owns a Wearable, 1 in 10 Wears Them Daily*, MOBIHEALTHNEWS (Oct. 21, 2014), http://www.mobihealthnews.com/37543/pwc-1-in-5-americans-owns-a-wearable-1-in-10-wears-them-daily.

36. Gary Marshall, *The Story of Fitbit: How a Wooden Box Became a $4 Billion Company*, WAREABLE (Sep. 9, 2016), http://www.wareable.com/fitbit/youre-fitbit-and-you-know-it-how-a-wooden-box-became-a-dollar-4-billion-company (noting that Fitbit was founded in 2007); *see also* Leibenger et al., *supra* note 14, at 315 (noting that the term "quantified self" first arose in 2007).

trackers has taken place on such a large and expedited scale that it has, in many ways, far escaped social contextualization. Instead of being digested by and normalized into existing social structures—with their built-in norms that outline approved actors, information flows, and dissemination principles[37]—self-quantification data has been *acting upon* those structures—generating new flows and breaking down or redrawing contextual boundaries.[38] Such an impact is due in part to empirical reality—technological change outpacing and serving as a historical precipitator of sociocultural change—and in part to its characteristic mode of production. As highlighted above, the unifying feature of this type of data is its collection by and for the self. By its very nature, then, self-quantification data is generated asocially. Of course, it is created in a highly web-connected environment and can be shared easily and seamlessly, but crucially, this type of data's key defining feature is its "selfie-ness." Unlike the central health data case, which revolves around the clinical setting, it is not generated within a social context.[39] Indeed, one of its most innovative aspects is the extent to which it *dispenses* with a social context that may have previously been necessary to the revelation of certain sorts of data. Athletes used to need coaches and assistants with timers and stopwatches and cameras. Poor sleepers used to need medical students at sleep clinics. But now they are liberated. Now they can track their own behaviors without being required to enter into a particular social setting—they can get the information without the context. Self-quantification data is decontextualized.

This individualized data may come without a context, but it does not come without a construct. And the accompanying technological construct—data storage, data anonymization and analysis, and data transmission to commercial vendors and other third parties—enables self-quantification data to be leveraged in a variety of contexts toward a variety of ends. Historically speaking, the first and most prevalent set of actors to attempt to exploit this data's technological construct, in the United States, has been employers.[40] Employer efforts to capitalize on

---

37. *See* Nissenbaum & Patterson, *supra* note 28, at 82.

38. *See* Kang et al., *supra* note 12, at 823.

39. Patterson, *supra* note 22, at 19-20 (quoting FOOD & DRUG ADMIN., DRAFT GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF, MOBILE MEDICAL APPLICATIONS 11 (July 21, 2011) (updated by MOBILE MEDICAL APPLICATIONS, *supra* note 24)).

40. *See* Alexandra Troiano, *Wearables and Personal Health Data: Putting a Premium on Your Privacy,* 82 BROOK. L. REV. 1715, 1717 (2017); *see also* Parmy Olson, *Fitbit's Game Plan for Making Your Company Healthy*, FORBES (Jan 8, 2016, 2:52 PM), http://www.forbes.

the proliferation of self-quantification data by incorporating wearable personal fitness monitors into corporate wellness programs bring decontextualized data into a very particular context, giving rise to a host of concerns that have been identified mainly through the lens of privacy but that also relate to autonomy and equality interests.

1. Self-Quantification Data in the Workplace

There are several mechanisms through which self-quantification data typically enters the workplace, each of which have been highlighted in the existing literature.[41] The first is incentivized sharing, whereby employees disclose their data to employers in return for some sort of benefit, typically as part of a voluntary wellness initiative.[42] Often in such scenarios, the devices are employer-provided or discounted,[43] offered to those employees who wish to participate in office-wide competitions designed to spur healthier lifestyles and cut down on insurance costs.[44] Employees may opt in to get the device for free, out of a sense of peer pressure, or because companies promise them lower health-care costs.[45] Fitbit sells its devices to employers, and one research firm has estimated that 10,000 U.S. companies offered fitness trackers to their staffs in 2014 alone.[46] By 2016, Fitbit counted numerous multinational corporations among its clientele, including BP, Bank of America, IBM, Time Warner, Target, and Barclays.[47] Similar programs employ a bring-your-own-device (BYOD) style, with participating employees enabling employer access to their personally purchased devices and voluntarily sharing the personal data produced in order to gain workplace benefits.[48]

---

com/sites/parmyolson/2016/01/08/fitbit-wearables-corporate-wellness/#a326e4b5ff60 (discussing Fitbit's active pursuit of the corporate wellness "market" since the company's 2009 inception).

41. *See* Ajunwa et al., *supra* note 11, at 475.

42. *See id.*

43. Christina Farr, *How Fitbit Became the Next Big Thing in Corporate Wellness*, FAST COMPANY (Apr. 18, 2016), http://www.fastcompany.com/3058462/how-fitbit-became-the-next-big-thing-in-corporate-wellness.

44. *Id.* (relating the details of BP America's Million Step Challenge, under which employees who reached step goals earned points toward lower-deductible health-care plans).

45. *Id.* (describing the particulars of various employee wellness programs, including those at IBM and at startup company Appirio).

46. Christovich, *supra* note 6, at 102-04.

47. *See* Farr, *supra* note 43.

48. Jonathan Edelheit, *Fitness Tracker Pitfalls*, CORP. WELLNESS MAG. (Aug. 7, 2015), http://www.corporatewellnessmagazine.com/column/wearable-device-pitfalls-is-this-wearable-fit-for-the-workplace/.

2. Concerns About Self-Quantification Data in the Workplace

For both such types of sharing, the concerns in the literature have been mostly privacy-oriented, although there are subtle variations.[49] With employer-sponsored devices, commentators raise the issue of whether the data stored there can even be considered private in the first place (although there seems to be a consensus feeling that it should be).[50] In the case of BYOD initiatives, there is a stronger sense that the generated data is private to begin with.[51] However, there is nevertheless a persistent concern that entangling this data with the workplace robs it of the privacy protections that should self-evidently attach.[52] For example, Elizabeth Brown notes that "[w]hen employers give their employees electronic devices . . . the employers arguably have greater legal access to the data on those devices than anyone else."[53] She uses this insight to draw attention to the lacuna such data occupies in the U.S. legal framework—the reality that employees who share a wealth of personal wellness data via employer-provided devices likely lack a reasonable expectation of privacy in such sensor-generated data, meaning that they will not have any legal ground from which to complain about employer misuse of their information.[54] Ifeoma Ajunwa, Kate Crawford, and Joel Ford echo this concern about the thorny contextual issues surrounding corporate wellness programs:

> Many wellness programs employ electronic wearable fitness devices, and if these devices are owned by the employer, then any data collected from them may legally also be the property of the employer. But even beyond that, the law is not well settled that employees own and can control the usage of the data that are collected as part of wellness programs.[55]

Though the concern over mishandling or improper protection of self-quantification data is framed differently from the concern over ownership

---

49. *Compare* Ajunwa et al., *supra* note 11, at 477-78 (framing the operative issues raised by employee wellness program-based data sharing in terms of data *control* rather than mere privacy), *with* Christovich, *supra* note 6, at 100-12 (discussing "the heightened *privacy* concerns presented by the use of fitness trackers") (emphasis added).

50. *See, e.g.*, Ajunwa et al., *supra* note 11, at 478 (recognizing that employee wearable data recorded by employer-owned devices might properly be considered the legal property of the employer, while simultaneously asserting that the employee should "retain[] control" of that data).

51. *See* Brown, *supra* note 8, at 16-19; *see also* Christovich, *supra* note 6, at 101.

52. *See* Christovich, *supra* note 6, at 101.

53. Brown, *supra* note 8, at 22-23.

54. *Id.*

55. Ajunwa et al., *supra* note 11, at 478.

of the raw information itself, both concerns are ultimately colored by the unspoken notion that employees should have the means to keep this information (which after all is made *about* them, *by* them) private; to keep it, so to speak, socially decontextualized. For instance, Brown goes on to highlight "the specific issue of employee privacy in health-related data collected from mobile sensors" before turning to federal health data regulations (like HIPAA and the Americans with Disabilities Amendments Act) to evaluate their potential application to such data.[56] Ajunwa's team, similarly, explicates a concern about employer ownership of self-quantification data in terms of the unforeseen privacy violations that will result when the selves generating the data do not own it: if employers legally own their employees' self-quantification data, employees "might find that [their personal health information] shared with an employer's wellness program continues to live on . . . long after [they have] left the firm."[57] Moreover, self-quantification data could flow to unforeseen parties in unforeseen ways, something that seems particularly shocking from within the viewpoint of the health data space, wherein such data is customarily treated as contextually bounded.[58] For instance, "such information could be sold . . . to entities far outside the realm of the employee's contemplation," an unacceptable outcome particularly because "joining a wellness program is an act of trust"[59] by which the employee brings his or her private data into the workplace for a specific purpose.[60]

Other concerns swirling around self-quantification data in the workplace are inflected with worries grounded in the concepts of autonomy, equality, or discrimination. For instance, many commentators point to the reality that fitness data—particularly when accompanied by the data mining and analytic capacities that already exist in the market—

---

56. Brown, *supra* note 8, at 23-24.

57. Ajunwa et al., *supra* note 11, at 478.

58. *See supra* Section II.A (discussing the central case of health data).

59. Ajunwa et al., *supra* note 11, at 478.

60. An additional interesting privacy-related concern articulated by Scott Peppet has to do with the way in which incentivized wellness data sharing in the workplace leads to a privacy "unraveling"—a process through which privacy context boundary lines are redrawn somewhat unintentionally, as a domino-effect consequence of incentivized sharing. *See* Peppet, *Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future*, 105 NW. U. L. REV. 1153, 1555-57 (2015); *see also* Christovich, *supra* note 6, at 104 ("Once a critical mass of employees begins voluntarily exchanging private health information for incentives through fitness trackers, it is probable that employers will assume that those who refuse to do so have something to hide.").

can be used to weed out costly employees.[61] Additionally, since general fitness itself is not in any way a protected characteristic,[62] employers are free to discriminate against the obese, or smokers, or simply those who like to keep their fitness activities out of the workplace.[63] Such concerns are magnified in the context of a third way in which self-quantification data can enter the workplace: mining by third parties and via other public sources.[64] Although a much less prominent means by which such data may enter the workplace—especially if wearable companies improve privacy practices[65]—it is possible for the data to make its way in unintentionally. If individuals share their data with their social networks, or otherwise in public or semi-public ways, employers may be able to discover it, and when such data is stored in the cloud, it can be subject to security leakage.[66] The privacy issues raised by this mode of intersection between self-quantification data and the workplace are more overt (as it is not characterized by conscious sharing), but the autonomy and discrimination issues are similar, and they are animated by a kind of contextual misplacement: Should employers be able to use this information in this way? Is it appropriate to deploy it within the workplace context?[67]

---

61. Ajunwa et al., *supra* note 11, at 478.

62. Christovich, *supra* note 6, at 97-98; *see also* Pasquale & Ragone, *supra* note 3, at 633, 637.

63. Brown, *supra* note 8, at 19-20 ("It is easy to imagine a scenario where an employer, having to decide which of two candidates to promote, reviews each candidate's sleep patterns, physical activity, calorie intake, or mood—any or all of which can be monitored and measured remotely—and decides based at least in part on these data. When employers use the health and fitness data they collect to make employment decisions, including hiring and promotion, there is cause for concern.").

64. *See* Pasquale & Ragone, *supra* note 3, at 632-37. Data mining refers to a variety of algorithmic techniques for drawing actionable insights from large datasets. *See generally* Alexander Furnas, *Everything You Wanted To Know About Data Mining but Were Afraid To Ask*, ATLANTIC (Apr. 3, 2012), http://www.theatlantic.com/technology/archive/2012/04/everything-you-wanted-to-know-about-data-mining-but-were-afraid-to-ask/255388/ (reviewing several types of pattern detection deployed in data mining, including anomaly and cluster detection, as well as classification).

65. Which they may be doing, perhaps in response to consumer concerns. Fitbit, for example, became HIPAA compliant in 2016. *See* Farr, *supra* note 43.

66. *See* Pasquale & Ragone, *supra* note 3, at 623-25, 631-50; *see also* Peppet, *supra* note 8, at 94-95; Catherine Clifford, *These Healthcare Data Companies Earn Millions by Making Employees Healthier, Saving Employers Boatloads of Money*, ENTREPRENEUR (June 3, 2016), http://www.entrepreneur.com/article/276807 (noting that third party analytics companies are mining employee health and health-adjacent data).

67. Of course, the irony is that the two previously explicated means of entry undermine privacy arguments relating to the third type. *See* Section II.C. The fact that employees are consciously and voluntarily bringing such information into the workplace themselves pulls the

Questions like this apply equally to the third and final type of data currently occupying the health and health-adjacent ecosystem, which I call "medical reputation data."

C. Medical Reputation Data—Interconnection and Inferences

In their 2014 article on health data privacy in the age of cloud computing, Frank Pasquale and Tara Adams Ragone use the term "medical reputation" to refer to a new sort of health-related data created by the collision of social science research and Big Data analytics.[68] Due to the wealth of non-health data existing in the broader datasphere, along with the growth of scientifically supported inferences connecting superficially unrelated data (as well as the fact that even anonymized data is increasingly easy to reidentify[69]), individuals now face issues with "health-inflected information [that can be used as the] source of correlations, profiles, and attributions."[70] If self-quantification data represents technology's capacity to produce socially decontextualized data, then the existence of medical reputation data demonstrates the way that it is rewriting or collapsing context altogether: by generating previously undiscovered inferences and allowing information to flow unbounded, Big Data is rendering privacy frameworks increasingly feeble.[71] As Pasquale and Ragone put it, "In an era of Big Data, companies do not even need to consult the 'health care sector' to impute various . . . conditions . . . to data subjects."[72] Other, health-inflected information—unprotected by the regulatory regime but previously kept out of the workplace by unspoken social-contextual boundaries—can enable employers to make reasonable inferences.

Medical reputation data, while perhaps also accurately described as health-adjacent, is different from self-quantification data in that rather than providing a wealth of granular detail that can generate a full picture of a person's behavior and biometric state, it is composed of only one or a

---

rug out from under arguments to the effect that such data should be, as a normative matter, separate from the workplace.

68. Pasquale & Ragone, *supra* note 3, at 629, 637.

69. *See* Peppet, *supra* note 8, at 94.

70. Pasquale & Ragone, *supra* note 3, at 633.

71. *See* Peppet, *supra* note 8, at 119-20 ("[S]ensor data tend to combine in unexpected ways, giving rise to powerful inferences from seemingly innocuous data sources. . . . Sensor data are so rich, accurate, and fine-grained that data from any given sensor context may be valuable in a variety of—and perhaps all—other economic or information contexts.").

72. Pasquale & Ragone, *supra* note 3, at 629.

few data points that are used to imply a pattern or support an inference.[73] Two examples are "allergy sufferers" or "dieters."[74] Records showing that an individual has bought over-the-counter allergy pills at several points in the past, or has responded positively to diet pill solicitations on a few occasions, constitute "health-inflected" data revelatory of wellness behaviors in a manner different from self-quantification data.[75]

The concerns revolving around such data both epitomize and reflect some of the broader issues with data mining, predictive analytics, and the Internet of Things[76]—including discriminatory uses and the sense of boundarylessness that deprives individuals of the space to autonomously make themselves.[77] Scott Peppet, for instance, complains that in an increasingly connected world "everything may reveal everything,"[78] and Robert Sprague worries that leveraging Big Data in this way codifies social biases.[79] For their part, Pasquale and Ragone worry that this sort of inference integration can result in "runaway data" that produces "cascading disadvantages"[80] for those whose health-inflected data falls afoul of corporate preferences.[81]

---

73. *See id.* at 630 (quoting Lois Beckett, *Everything We Know About What Data Brokers Know About You*, PROPUBLICA (Mar. 7, 2013), http://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you).

74. *See id.*

75. *See id.* at 632.

76. Predictive analytics refers to a type of data processing designed to "predict the future behavior of individuals in order to drive better decisions." Terry, *supra* note 17, at 77 (quoting ERIC SIEGEL, PREDICTIVE ANALYTICS: THE POWER TO PREDICT WHO WILL CLICK, BUY, LIE, OR DIE 11 (2013)). The Internet of Things refers to the increasingly encompassing "network connecting objects in the physical world to the internet." *See* Arik Gabbai, *Kevin Ashton Describes the* '*Internet of Things*,' SMITHSONIAN (Jan. 2015), http://www.smithsonianmag.com/innovation/kevin-ashton-describes-the-internet-of-things-180953749/. Everyday objects are increasingly produced with Internet connectivity capability, and so many household objects are beginning to be embedded with sensors enabling them to automatically transmit unstructured data to the cloud that a satirical Twitter account entitled "Internet of Shit" (documenting the silliness of some of the more "dubious" connectivity decisions) has emerged. Woodrow Hertzog & Evan Selinger, *The Internet of Heirlooms and Disposable Things*, 17 N.C. J.L. & TECH. 581, 582 (2016); *see* @internetofshit, TWITTER, http://twitter.com/internetofshit?lang=en (last visited Aug. 30, 2017).

77. In the Internet of Things with the Big Data filter, all data are "grist for drawing revealing and often unexpected inferences about our habits, predilections, and personalities." Peppet, *supra* note 8, at 90-91.

78. *Id.* at 93.

79. Sprague, *supra* note 3, at 35-37.

80. Pasquale & Ragone, *supra* note 3, at 632 (emphasis removed).

81. For instance, being a dieter could be linked to a bevy of health and psychological problems—diabetes, anorexia, bulimia, impulse control, etc.—or being an allergy sufferer could be linked to higher work absentee rates. *See* Peppet, *supra* note 8, at 119-20.

My map of the current health and health-adjacent data landscape thus includes three types of data, each of which hovers in this space for a matrix of reasons beyond the simple conceptual or taxonomic. These reasons include the historical but also the discursive and the social-perspectival. We are used to seeing this kind of information produced within and bounded by a particular social context, and as technology erodes or alters that context, we most often reach for privacy as a discursive and regulatory tool to reassert it. Especially as it pertains to intersection with the workplace, all of these types of data seem to exist within a web of related concerns; as such, their actual conceptual affinity is less important for the purposes of this Article than their treatment by the literature, which has been apt to discuss them together, as so many heads of a single, privacy-destroying Medusa.

Having set the stage with (1) the central case of health data, defined by its mode of production in a socially bounded context; (2) self-quantification data, decontextualized and yet presenting as similar and thus related to health data; and (3) medical reputation data, the offspring of Big Data's cross-contextualization, I will now introduce my conceptualization of a distinct yet associated type of data emerging within the ecosystem—what I call "productivity data."

III. PRODUCTIVITY DATA

A. Productivity Data Appears on the Scene

Workplace monitoring is nothing new. In his article *The Eavesdropping Employer*, Corey Ciocchetti chronicles the myriad of means by which employers have tracked employee behavior and output throughout recent history.[82] Moreover, ever since Frederick Winslow Taylor promulgated the *Principles of Scientific Management* in the early 20th century, corporate management has attempted to measure employees in order to routinize and optimize organizational productivity. But only now, with the advent of wearable sensors and data analytics, have these two aims—monitoring and management—found a harmonious and elegant application to the modern knowledge-based

82. Ciocchetti enumerates *thirteen* tactics, including: attendance and time monitoring; desktop monitoring; email monitoring; keystroke logging; use of filters and firewalls restricting Internet access; GPS, RFID and Smartcard usage; physical searches; telephone, text message, and voicemail monitoring; and video surveillance. *See* Ciocchetti, *supra* note 4, at 18-34.

economy.[83] The entry of wearable fitness devices into the workplace that began with health and wellness initiatives is now morphing into a happiness and productivity boosting regime that gathers, mines, and combines biometric and sociometric data to generate a "perfectly productive workplace."[84] This still-inchoate movement has been variously termed "the quantified self at work,"[85] "people analytics,"[86] and "the quantified workplace."[87]

Empirically, the growth of this type of measurement—which I'll refer to here as "productivity monitoring"—derives from the expansion of sensor technology.[88] Historically, the intersection of sensor technology and the workplace has come in the form of wearable fitness.[89] This confluence of events has yielded a state of affairs in which productivity monitoring is inextricably linked with self-quantification. Indeed, much of the popular coverage of the phenomenon treats the productivity movement as an evolution of self-quantification that deepens and contextualizes the social-psychological profile of the individual in the context of his or her job performance. Consider this *Tech Republic* article from 2016, which describes the "road to employee monitoring" and the "biometric CV" as beginning with the ascendance of fitness monitoring bands like Fitbit "generally aimed at individuals who want to improve their health" and as now giving way to attempts to exploit

---

83. The concept of the knowledge-based economy emerged in the mid-twentieth century as a means for describing the "expansion of knowledge-intensive industries and the accompanying productivity increase" within the context of certain advanced economies. Walter W. Powell & Kaisa Snellman, *The Knowledge Economy*, 30 ANN. REV. SOCIOL. 199, 200 (2004). In the United States, it suggests the notion that "key sectors of the economy are more reliant on knowledge generation and dissemination today than" they once were. *Id.* at 201.

84. Brett Frischmann & Evan Selinger, *Utopia?: A Technologically Determined World of Frictionless Transactions, Optimized Production, and Maximal Happiness*, 64 UCLA L. REV. DISCOURSE 372, 378 (2016).

85. Wylie Wong, *Want To Improve Employee Efficiency*? *Wearables Could Be the Answer*, BIZTECH (Feb. 10, 2017), http://biztechmagazine.com/article/2017/02/want-improve-employee-productivity-wearables-could-be-answer.

86. Josh Bersin et al., *Will IoT Technology Bring Us the Quantified Employee*?: *The Internet of Things in Human Resources,* DELOITTE (May 24, 2016), http://dupress.deloitte.com/dup-us-en/focus/internet-of-things/people-analytics-iot-human-resources.html#endnote-sup-11.

87. Phoebe Moore & Lukasz Piwek, *Regulating Wellbeing in the Brave New Quantified Workplace*, 39 EMPLOYEE RELATIONS 308, 309 (2016).

88. *See* Peppet, *supra* note 8, at 92-93; *see also* Daniel Burrus, *The Internet of Things Is Far Bigger than Anyone Realizes*, WIRED (2014), http://www.wired.com/insights/2014/11/the-internet-of-things-bigger/.

89. *See supra* Part II.

"wearable data to improve staff productivity."[90] The article goes on to introduce some of the accompanying technology that expands upon wearable sensor data to provide management insights by discussing and explaining the mission of BioBeats, a startup that, in 2016, was attempting to locate the optimal level of stress for financial traders (whose job performance often revolves around making appropriately risky decisions within a hectic environment) by deriving information about stress from "patterns in physiological data such as heart rate variability."[91] Or consider a *BizTech* article from early 2017 that uses the lead line "fitness trackers find a home in the workplace" as an entry into coverage of the way in which companies are beginning to "equip employees with wearable sensors that track their movements and speech patterns" in order to uncover "trends and make adjustments aimed at boosting performance"—for instance by "redesigning office spaces to encourage communication and collaboration."[92] Thus, productivity monitoring is linked to self-quantification; it is interested in all of the biometric measurements that movement has to offer, but it extends beyond them to consider the totality of conditions for success in the workplace.

Before turning to my formulation of productivity data, I offer a few examples of the types of measurements representing the incarnation of this movement.

B. Versions of Productivity Monitoring

Perhaps the most popularly reported instance of productivity monitoring to date is Sociometric Solutions's work with Bank of America in 2009, in which the company deployed wearable devices to employees of a Rhode Island call center.[93] The devices included microphones, Bluetooth transmitters, motion sensors, and infrared beams and were used to monitor where employees went, who they spoke with, and how the "tone of voice and the movements of their bodies changed throughout the day."[94] Using this data, the tech company was able to discern that

---

90. Nick Heath, *Every Step You Take: How Wearables Will Help the Boss Keep Tabs on Staff*, TECHREPUBLIC (Apr. 11, 2016, 8:16 AM), http://www.techrepublic.com/article/every-step-you-take-how-wearables-will-help-the-boss-keep-tabs-on-staff/.

91. *Id.*

92. *See* Wong, *supra* note 85.

93. Aviva Rutkin, *Wearable Tech Lets Boss Track Your Work, Rest and Play*, NEW SCIENTIST (Oct. 15, 2014), http://www.newscientist.com/article/mg22429913-000-wearable-tech-lets-boss-track-your-work-rest-and-play/.

94. *Id.*

socially engaged employees were more productive—ultimately clearing more calls.[95] This somewhat counterintuitive insight spurred the company to alter break structure and tweak office culture.[96] As the very name of the company implies, Sociometric Solutions uses wearable sensors to measure the social dimensions of the workplace environment, with the aim of discerning the social conditions most likely to foster productivity.[97]

Another famous example is Hitachi's happiness-measuring badges, which, similarly to those utilized by Sociometric Solutions, collect data about employee movements throughout the day, including amount of time spent "sitting, walking, nodding, typing, and talking."[98] The company uses these measurements to derive information about the workforce's overall organizational activity level, which includes information about the variety and length of in-office communication and about solitary, sedentary time.[99] The company then feeds the data into its proprietary model for optimal workplace "happiness"—which is presumably some "just right" activity level—in order to inform workforce management decisions.[100] Under this formulation, activity level reflects and/or creates happiness, and happiness, in turn, generates productivity.[101] Thus, this incarnation of productivity monitoring makes happiness a condition for workplace success, meaning that employers are interested both in fostering and in measuring it.[102]

A final, and somewhat different example, pertains more directly to the measurement of what an article from the *Harvard Business Review*

---

95. *Id.*; *see also* Joshua Rothman, *Big Data Comes to the Office*, NEW YORKER (June 3, 2014), http://www.newyorker.com/books/joshua-rothman/big-data-comes-to-the-office (relaying the fact that the use of the sociometric badges revealed that the most competitive Bank of America call center team—the one with the highest "A.H.T." (average call handling time)—was also the one whose members spent the most time chatting with each other).

96. *See* Peppet, *supra* note 8, at 113; *see also* Stuart Frankel, *Employers Are Using Workplace Wearables To Find Out How Happy and Productive We Are*, QUARTZ (Aug. 11, 2016), http://qz.com/754989/employers-are-using-workplace-wearables-to-find-out-how-happy-and-productive-we-are/; Rothman, *supra* note 95 (explaining that when Bank of America introduced "team-wide coffee breaks, designed to encourage mingling . . . at all of its call centers," this change generated a "fifteen-million-dollar increase in annual productivity").

97. Rob Matheson, *Moneyball for Business: Startup's Behavioral Analytics on Employees Uncover Ways To Increase Workplace Productivity, Satisfaction*, MIT NEWS (Nov. 14, 2014), http://news.mit.edu/2014/behavioral-analytics-moneyball-for-business-1114.

98. Frankel, *supra* note 96.

99. Tsuji et al., *Use of Human Big Data To Help Improve Productivity in Service Businesses*, 65 HITACHI REV. 847, 848 (2016).

100. *Id.*

101. *Id.*

102. *Id.*

calls "the big data inside us."[103] This type of productivity measurement actually tracks knowledge production and is epitomized by Melon's wearable EEG headband, which is designed to "help wearers understand their cognitive patterns" by charting "the spikes in gamma brain waves that occur milliseconds before an 'aha' moment," with the aim of determining (and, perhaps in the future, deducing how to *induce*) when individuals "are likely to be most creative."[104] As one commentator puts it, this type of measurement aims to quantify "the physiological functions, from the movements of our hearts to the firings of the neurons in our brains, that underlie how we work."[105]

Taken together, these examples demonstrate the development and contours of productivity data, which combines both individual, internal measurements and external, social measurements to create a full picture of the conditions underlying knowledge production. My proffered definition accounts for these contours.

C. Productivity Data Defined—the Features of Productivity Data

> **Productivity Data:** any and all data relating to the individual, psychological, physiological, social, and/or environmental conditions underlying the production of knowledge, innovation, and/or creativity

Productivity data encompasses all types of information collected in order to generate a comprehensive picture of the optimal conditions under which knowledge is produced. It can be thought of as having several defining features: it is integrative, interactive, and designed to be exploitable. Examining these features against the backdrop of the ecosystem map created in Part II will allow expansion on the above definition and will provide insight into the ways that this kind of data is both related to and distinct from the other extant types.

---

103. H. James Wilson, *Wearables in the Workplace*, HARV. BUS. REV. (Sept. 2013), http://hbr.org/2013/09/wearables-in-the-workplace.

104. *Id.*

105. *Id.* *See* Rohit Sharma et al., *Physiolytics*: *Improving Workplace Efficiency* slide 2 (Apr. 14, 2014), http://www.slideshare.net/hailderon/physiolytics; *see also What Is Physiolytics*?, PHYSIOLYTICS LABORATORY, http://physlyt.com/what-is-pysiolytics/ (last visited Oct. 18, 2017). To describe this type of measurement, Wilson used the term "physiolytics," which has been defined as the "practice of linking wearable computing devices with data analysis and quantified feedback to improve performance." Wilson, *supra* note 103.

To begin with, productivity data is integrative. While it can encompass self-quantification-type data having to do with individuals' physical and biometric markers, whether the data is self-collected (transmitted to employers) or employer-collected, its aim is to integrate such data within a broader social-psychological context to generate insights about how knowledge is created. So, for instance, a basic productivity data collection regime in the workplace would be multifaceted, possessing at least two measurement metrics: personal biometric markers and "work-computer-based" or sociometric tracking of the type explained above.[106] Such measurements would then be integrated to create a fuller productivity picture. Consider this example, drawn by Phoebe Moore and Lukasz Piwek:

> [E]very employee working for a company is wearing a . . . [personal fitness tracking device that tracks] movement, heart rate, proximity to other employees, body temperature, and skin conductance. Simultaneously, every work-computer-based activity is also tracked in par with the wearable device. Data from both wearable devices and work computers is wirelessly uploaded to a central system. The system provides detailed personal analytics for each employee: levels and suggestions for physical activity, indicators of stress, productive and sedentary periods at work, work-based social interaction patterns . . . . All the data are synchronised with individual calendars and planners, with e-mail systems and individually tailored virtual encouragement and performance dashboards.[107]

Such data, then, is collected within an integrated system. While certain of its components resemble or appear identical to self-quantification data, productivity data relates those components to the knowledge-production project and is interested in how they can be integrated with other social, psychological, and environmental elements. This means that productivity data hovers in the health and health-adjacent data ecosystem because, as a definitional matter, it can and does encompass bits of information that we currently find in this space: data concerning mental states, emotional moods, and exercise levels can all be part of an integrated picture of productivity. Indeed, the discourse surrounding personal fitness trackers in the workplace reflects the existing, often unspoken management assumption that "[w]ellbeing is . . . linked to

---

106. *See supra* Sections II.A-B. The phrase "work-computer-based" is taken from Moore & Piwek, *supra* note 87, at 308.

107. Moore & Piwek, *supra* note 87, at 308.

productivity."[108] Although the notion that "happy," "fit" workers are more innovative or efficient in terms of knowledge production is certainly contestable,[109] it represents a working assumption of the productivity measurement movement, which aims to integrate workplace monitoring with biometric monitoring to provide "insights into how to manage time and identify productive periods."[110]

Productivity data is also interactive. This means two distinct things. First, it means that productivity data is designed to reflect metrics of employee interaction with one another and with the physical environment, most typically environments within the workplace but also any other environments that feed into employees' integrated profiles and that they therefore bring with them to their production of knowledge. The type of data collected by Sociometric Solutions or Hitachi's happy badge provide examples: this sort of location and movement tracking, which is designed to "gather real-time information on how teams of employees work," is the most prominent of the currently nascent productivity data movement.[111] Self-quantification devices can also track movement and collect mobility data.[112] While that may present certain privacy concerns, it is often the least invasive or worrisome type of such data from a health data perspective. Yes, it can provide a privacy-invading portrait of how an individual is living his or her life and reveal doctor or clinic visits,[113] but such data is perhaps the least closely "health" related of all the data collected by wearable fitness devices.[114] From a

---

108. This is a clear example of slippage in our sociocultural notions in the wearable space. Wearables can and do increase productivity in the manufacturing and logistical space—for instance by automating inventory processes—and employee absenteeism due to illness can drive down productivity in the knowledge-based economy. However, it is certainly the case that we may have overburdened the connection between wellness and productivity beyond the more stable, elementary notion that being at work = being productive to the more subtle, slippery assumption that being healthy, happy, and well = being productive. *See generally* Wilson, *supra* note 103 (discussing other uses of wearables in the office to increase productivity that are not associated with health and/or wellness).

109. *See* Moore & Piwek, *supra* note 87, at 312.

110. *Id.* at 311.

111. Peppet, *supra* note 8, at 112; *see also* Claire Zillman, *Here's Yet Another Way Your Boss Can Spy on You*, FORTUNE (Jan. 13, 2016), http://fortune.com/2016/01/13/employee-surveillance-motion-sensors/ (detailing the Occupeye monitoring device, which uses heat and motion sensors to determine whether space is occupied, and has been deployed in the workplace to gather data about how employees utilize workspace).

112. *See* Brown, *supra* note 8, at 8.

113. This is particularly worrisome for women, who express concern about location data being released and the potential for violent stalking. *See* Patterson, *supra* note 22, at 45.

114. For instance, compare location and movement data with heart rate or sleep pattern data: while the latter reflects information often associated with the clinical medical context—

productivity data perspective, however, this kind of data might be particularly revelatory: Sociometric Solutions claims to be able to "divine from a worker's patterns of movement" such things as whether an employee will be promoted or whether a workplace team will win a contest.[115]

Characterizing productivity data as interactive also means that it has a somewhat complex relationship to context. Such data can be and often is contextual in that it represents quantification of the environmental, social, and even spatial contexts where knowledge is produced. But it can also be individual in the sense that it measures only a single person's psychological profile, or his or her brain wave activity. Productivity data can encompass self-measurement that is brought into the workplace voluntarily, measurements of the self *in* the workplace, and measurements of the workplace itself, as it is created by hierarchies, spatial designs, cultural policies, or normative rules. In other words, productivity data should be understood as concerned with context but not bounded by it. Data concerning any social context related to knowledge production can qualify, but cross-contextual biometric data, which exists as an aspect of individuals and follows them from context to context as they live their lives, is also desired. If something happening at home is making an employee tired or depressed at work, productivity data is keen to uncover that.

Finally, productivity data is meant to be exploitable. It is meant to harness the power of data to assist in the generation of a particular outcome. While all data is, in essence, a tool to be used to accomplish some end, productivity data is noteworthy for the way in which it attempts to open new data pathways between previously separated social contexts in order to exploit data from one context toward an outcome in what may have traditionally been considered an unrelated context. Productivity data epitomizes the entire thrust of the Big Data project in this sense—it is integration aiming to derive knowledge almost out of thin air, a project that seems at once utterly rational and eerily reminiscent of Rumpelstiltskin. Its exploitative bent is also what makes productivity data problematic in the health data space, and perhaps an

---

because, historically, it has either routinely or exclusively been measured within that context—the former lacks close affiliation with the medical context, and may more often be considered within the surveillance context. *See supra* note 16; *see also supra* Section II.A.

115. Peppet, *supra* note 8, at 114 (quoting Rachel Emma Silverman, *Tracking Sensors Invade the Workplace*, WALL ST. J. (Mar. 7, 2013, 11:42 AM), http://www.wsj.com/articles/SB10001424127887324034804578344303429080678).

aspect that drives much of the fraught feeling about it, in both the scholarly and the broader popular cultural worlds. As noted in Part II, the central case of health data is defined in large part by our social contextual markers: such data is generated in the context of a confidential relationship, the purpose and meaning of which is relatively settled and accepted. True health data occupies a specific social sphere that is meant to stand alone; the information produced within it is not meant to flow freely to other social contexts. Self-quantification data moves some of this type of data beyond the central definitive social context, a movement that is already fraught, but that we as a society have mostly normalized by decontextualizing the information: self-quantification data might be health data, and to the extent that it is, it is at least not moving into other social contexts but is instead remaining under the purview of the individual. This, in turn, may be why the privacy perspective feels so applicable when it comes to dealing with self-quantification data, and why so much of the literature[116] revolves around the exact calibration of privacy regulation appropriate to such data.[117] We may accept data moving beyond the context of its creation, but we are not entirely comfortable with its moving into a new context, where it might take on a different, unanticipated, or unwelcome meaning. Productivity data, for its part, begins to give shape to what it means for social contextual boundaries to break down in the face of Big Data. It involves data that originates outside the confines of the workplace but nevertheless represents information and provides insight into the conditions for knowledge production. Whilst the social meaning of pure health data has, in the past, been characterized by market inalienability,[118] productivity data treats the same bits of data as exploitable, as efficiency-generating and potentially wealth-creating.

Even though the movement itself is still in its early stages, and may in the end be stymied by political, sociocultural, or legal forces, I believe that it is this disquiet about data dis- or mis-placement that underlies much of the hand-wringing regarding health and health-adjacent data in the workplace. But while focusing on the more prominent categories of health data and self-quantification data can make a focus on privacy problems seem natural and inevitable, examining productivity data, which is evolving in this space and often being treated as part and parcel

116. *See supra* Part II.

117. *See supra* Parts I & II.

118. *See* Margaret Jane Radin, *Market Inalienability*, 100 HARV. L. REV. 1849, 1849 (1987).

of the wellness trend, reveals some considerations that have heretofore been overlooked. Namely, carving out this type of data uncovers the human capital dimensions of the quantification-in-the-employment-context problem. These are concerns that privacy solutions cannot and will not entirely respond to, and their existence suggests the importance of broadening the perspectives from which both legal scholarship and social commentary approach the issue.

IV. CONDITIONS FOR GENERATING KNOWLEDGE HAVE ECONOMIC VALUE: INTRODUCING THE HUMAN CAPITAL LAW LENS

The notion of human capital was promulgated most recently and comprehensively by the economist Gary Becker in the middle of the twentieth century, but the concept itself dates back at least to Adam Smith.[119] Broadly speaking, it relates the idea that a variety of different kinds of investments in people—the components of the labor force—contribute to the production of knowledge and thereby possess economic value.[120] The most common examples are education, professional training, and health care; but Becker also includes "the influence of families on the knowledge, skills . . . values, and habits of their children."[121] Other theorists also reference talent and expertise,[122] demonstrating that the concept is malleable, with space to include a variety of factors capable of contributing to knowledge production. The key defining feature of human capital is its inalienability—while capable of producing economic value, it cannot be separated from individuals in the way that other assets can.[123] As Peter Fleming puts it, "[T]he individual cannot be separated from his human capital."[124]

While the many nuances of the economic theory fall beyond the purview of this Article, the relationship between human capital and productivity data should be readily apparent. Understood in context, productivity data can be thought of as attempted quantification of certain human capital intangibles on a granular level; it charts a variety of data

---

119. Claudia Goldin, *Human Capital*, *in* HANDBOOK OF CLIOMETRICS 55, 56 (Claude Diebolt & Michael Haupert eds., 2016), http://scholar.harvard.edu/files/goldin/files/goldin_humancapital.pdf; *see* Gary S. Becker, *Human Capital*, *in* THE CONCISE ENCYCLOPEDIA OF ECONOMICS (David R. Henderson ed., 2d ed. 2007), http://www.econlib.org/library/Enc/HumanCapital.html.

120. Goldin, *supra* note 119, at 56.

121. Becker, *supra* note 120.

122. Goldin, *supra* note 119, at 83.

123. *Id.*; *see also* Fleming, *supra* note 2.

124. Fleming, *supra* note 2.

metrics concerning the conditions under which human capital generates value, attempting to capture them as a means for achieving optimal exploitation.[125] Tracking health, psychological, and mood data might yield insight into how exactly individual health translates to corporate value. Similarly, measuring brain waves might yield specific conclusions about the way in which education translates into innovation. In this way, focusing on the productivity monitoring movement shifts the contours of the health and health-adjacent data debate to a framework beyond privacy. One's health data does not draw legal protection only as a dignitary matter but also as a means to prevent exploitation. Such data does not just belong to a person in the sense that he or she should be able to control who knows it and when but also in the sense that, to the extent it is exploitable, that individual should reap the returns. Examining the issue from this perspective introduces alternative considerations and solutions that the privacy perspective fails to illuminate—namely, it highlights the reality that concerns around health-adjacent data entering the workplace in the modern knowledge economy may involve propertization and ownership just as much as (if not more than) privacy. To see how this is the case, we need look little farther than the appeal of the consumer self-quantification movement itself, which is composed of individuals leveraging "intimate data generation techniques" for their own personal gain: people can "explore various aspects of [their] 'autonomic selves' . . . that would not otherwise be knowable," and use the information to "improve work habits" or reach personal sporting and/or fitness goals.[126]

If the struggle over health-adjacent data in the workplace is reconceived as one about where to direct the human capital dividends, then we are faced with a different sort of legal question from those that have already been asked, which mostly revolve around ensuring that personal data is secured and controlled[127] by those who produce it. Such new questions are, instead, about whether data-producing individuals can wield the primary power to exploit their productivity data or otherwise

---

125. *See supra* Part III.

126. Moore & Piwek, *supra* note 87, at 311.

127. I use the notion "control" here to convey the sense that the productive individual is entitled to control the contextual flows of his or her information, borrowing somewhat from Kang et al.'s ideas in *Self-Surveillance Privacy*. *See* Kang et al., *supra* note 12, at 821. While it is clear that the notion of privacy as control has crossover with the notion of data control as economic ownership, most uses of the privacy-as-control notion in the health-adjacent data context have not encompassed the latter meaning, which I specifically refer to, and which I treat as being defined by its capacity for economic exploitation in the knowledge economy.

share in the economic value it generates in the knowledge economy and about how to design a legal regime that appropriately organizes such capital. In order to understand both how to formulate these questions and how to offer solutions to them, we should look to the existing web of contractual, employment, and intellectual property law rules that currently regulate human capital.[128]

A. Cognitive Propertization—the Current Trend of Human Capital Law

In her 2015 article *The New Cognitive Property: Human Capital Law and the Reach of Intellectual Property*, Law Professor Orly Lobel introduces "the growing field of human capital law," which exists at the intersection of "IP law, contract and employment law, and antitrust law."[129] Human capital law describes how the modern prevalence of a variety of "regulatory and contractual controls on human capital" is leading to what Lobel calls the "Third Enclosure Movement."[130] Through this movement, human capital and other "intangibles of the mind"—like knowledge, experience, skill, and creativity—are increasingly propertized.[131] According to Lobel, the contractual tools deployed to control capital in the modern knowledge economy workplace—things such as pre-innovation assignment agreements, nondisclosure agreements, non-competes, non-dealing clauses, and non-solicitation agreements—have begun to metastasize.[132] Such unchecked expansion both undermines the balance struck by IP law and also swallows innovation, and the *potential* for innovation, in a way that increasingly alienates humans from their capital.[133] Surprisingly or unsurprisingly, this trend is particularly acute in the tech industry, a field from which Lobel draws some of her most illustrative case studies.[134] Here, employee contracts routinely assign ownership—and thus, exploitative power—over any and all intellectual labor to the employer—whether such labor is propertizable according to IP law or not.[135] Thus, the employment market is increasingly treating human capital components as alienable even

128. This discussion is focused on U.S. law.

129. Orly Lobel, *The New Cognitive Property: Human Capital Law and the Reach of Intellectual Property*, 93 TEX. L. REV. 789, 790 (2015).

130. *Id.* at 790-93.

131. *Id.* at 793-95.

132. *Id.* at 791.

133. *Id.* at 793-96.

134. *Id.* at 803-32.

135. *Id.* at 797-821.

where the legal regime does not, employing the alternative mechanism of contract law to reshape the contours of the legal landscape and create ownership rights where there were none before.[136]

Consider the following example, which reflects the context collapse endemic in the modern professional workplace. Employees who work for knowledge-based companies often sign, as part of their employment agreement, assignment clauses, which transfer to their employers the IP rights over all innovation they perform in the scope of employment.[137] Now, as innovation becomes some of the most valuable of all human capital, and the workplace becomes a 24/7 endeavor, such clauses are being expanded in time and scope and also becoming increasingly unnecessary thanks to the changing nature of work.[138] When employees are hired to invent, and almost all knowledge production can be deemed to be done in the scope of employment, contractual clauses most often act as a backstop to shore up employer rights claims.[139] Google's employment agreement, for instance, "explicitly encompasses weekends and nights in its standard assignment agreement," which states that "Google Inc. will own all Inventions that I invented, developed, reduced to practice, or otherwise contributed to, solely or jointly with others, during my employment with Google (including during my off-duty hours)."[140] If you go to work for Google, then, any and all the knowledge you produce while in their employ is theirs to exploit, even if it represents the culmination of a lifetime of self-investment in education, research, and idea development[141]—even if, in other words, it derives from what is rightly considered to be your human capital. There is, of course, nothing inherently wrong with such a state of affairs. Individuals are and should be perfectly free to alienate their human capital in ways they see fit, including via contract. But Lobel's painstakingly argued point is that this enclosure movement "which strips employees [of] their ownership over their human capital" is not happening via democratic restructuring of public institutions.[142] Instead, it is being more subtly accomplished by employers through the use of private contract law without attracting

---

136. *Id.* at 834.
137. *Id.* at 812-21.
138. *See id.* at 820-25.
139. *Id.*
140. *Id.* at 823-24 (quoting source of Google Employment Contract, Cal. Ed. 2014 (on file with author)).
141. *Id.* at 813-15 (providing one example of the way in which innovation can represent the culmination of long-term knowledge work).
142. *Id.* at 839.

much attention from the policymakers who shape legal regimes.[143] As the legal scholars and policymakers debate and broker privacy solutions,[144] industry is rewriting the ownership rulebook right under our noses. Maybe, if we just wanted to keep our productivity and other health-adjacent data decontextualized, this would not be worrisome. But if, as this Article suspects, our concerns with such data are motivated, at least in part, by human-capital-infused ideas about the potential for exploitation, we would do well to heed Professor Lobel's warning note.

B. Defining the Human Capital Law Lens

Examining productivity data through the lens of human capital law shifts our attention to a different set of concerns than those raised when this data is considered through the lens of health. By helping us to get out of the health space, it illuminates ways of thinking about such data that are not bogged down in the baggage of the privacy debate. There are three aspects of the human capital law lens that are particularly helpful in this respect: its workplace orientation, its market exchange-based logic, and its focus on industrial patterns.

To begin with, the human capital law lens puts the focus squarely on the employment relationship. This is a sort of reversal of the current trend in the literature, which often treats the workplace as secondary to the reality of an expansion of health and health-adjacent data.[145] Scholarly articles talk about what privacy one has for his or her data *when it comes* to the office, and popular articles reference the productivity monitoring trend as an outgrowth of self-quantification.[146] What these approaches have in common is that they treat the health or health-adjacent—the personal, individualized nature of the data—as primary, asking what privacy protections it should attract when it comes into the workplace.[147] The human capital law lens, in contrast, does not treat the employment context as subsidiary; instead, it treats the contours of the employment relationship as a starting point, examining where they are being drawn empirically and asking where they should exist normatively. In other words, the human capital law lens looks to the

---

143. *Id.* at 797 ("Each of these [contractual] mechanisms, vigorously employed by companies to propertize human capital, is subject to doctrinal rules and litigation, but has received surprisingly little attention as a field of law.").

144. *See supra* notes 3-18 and accompanying text.

145. *See supra* Part II.

146. *See supra* Section II.A-C.

147. *See supra* notes 3-18 and accompanying text.

workplace first and asks where it might be said to end and what it might be said to include in a modern knowledge economy, especially in light of the disappearing physical and social boundaries between work and nonwork life. This shift forces us to consider a reality that the privacy perspective would like to turn a blind eye to: the fact that much of our personal data has already irretrievably escaped our grasp—it is out there; it is not private; in truth, the fact that it exists at all is often a sign that it has already been alienated from us. A workplace-oriented lens helps us to ask questions other than how we can put the genie back in the proverbial bottle.

Secondly, the human capital law lens adopts a market-exchange-based logic, meaning it focuses on the economic value of health, health-adjacent, and productivity data. It asks whether and how this kind of data can be exploited, as well as about the social desirability of such an outcome. If the workplace orientation of this alternative lens forces us to see that perhaps this data is already being leveraged for value in the workplace, its market logic nudges us to consider whether we want this to be the case. The question of the desirability of making such data market alienable brings with it accompanying issues about how to allocate the economic value that it creates. As Peter Fleming puts it in the quote at the beginning of this Article: because the key defining feature of human capital is its inalienability, "who exactly ought" to reap its benefits?[148] The human capital law lens encourages us to ask questions that seem, from a privacy perspective, at best irrelevant and at worst quite gauche. But they are questions that lurk in the reality of the productivity monitoring movement nonetheless: questions about whether your data is yours to exploit, whether your employer may not be just violating your privacy but stealing from you, and whether the office's attempt to quantify employees is actually a way of harvesting their capital.

Finally, the human capital law lens is focused on industrial patterns. A large part of Lobel's project in drawing the contours of this field is to demonstrate the way in which industry practices with regard to human capital undermine existing intellectual property structures.[149] Applying this kind of insight to productivity data in the health and health-adjacent field asks us to consider how industry is treating such data and evolving in response to its collection. Rather than conceptualizing the issue as one

148. *See supra* note 2 and accompanying text.
149. *See* Lobel, *supra* note 129, at 791-93, 840-47.

in which employers are increasingly invading a posited, preexisting private sphere, this lens shifts the focus to the structures that compose the employment relationship itself and encourages us to deal with them *directly*, rather than understanding them as incidental to a more important privacy regime.[150] Professor Lobel, for instance, suggests that trends in the human capital law realm indicate an industry-wide movement to "propertize" all human knowledge.[151] Following her lead as it pertains to the rise of self-quantification data in the workplace and the emergence of the productivity monitoring movement, it is possible to suggest a simultaneous trend toward the "datafication" of knowledge, designed to make the conditions for its production quantifiable and reproducible.

Examining productivity data through the lens of human capital law raises different concerns from those that have heretofore preoccupied scholars and commentators. It shifts the focus away from privacy and opens up alternative metrics for conceptualizing and treating heath-adjacent data in the age of Big Data. Such a shift is valuable, not because the privacy discussion is unimportant, but because as the types of data within this ecosystem evolve and move progressively further away from the central case, the circumstantial/historical entanglement of such data with privacy may over-determine the conceptual framing. Bringing an exploitation metric into the mix will help to obviate such accidental narrowness.

For each of these reasons, human capital law is a useful lens for examining productivity data. In the next Part, I will highlight several of the lessons its application can provide.

V. LESSONS FROM THE HUMAN CAPITAL LAW LENS

Having introduced the concept of productivity data and defined the human capital law lens as an alternative means for evaluating its impact on and import for the workplace, this Article will now sketch a few lessons that the application of the lens can bring to the current debate over health and health-adjacent data in the workplace.

150. *See supra* Part II.
151. Lobel, *supra* note 129, at 797.

A. Protection, Not Privacy

First, the human capital law lens demonstrates that the social meaning of the various types of data hovering in this space could be very different, despite their conceptual affinity to one another and to the notion of health. Because the social meaning of data has a large impact on the regulatory solutions offered to control and contain its use, applying the human capital law lens may aid in producing solutions that more closely track—or track differently—the social meaning of productivity data. To illustrate this idea, I have created a visual metric. In it, I have charted each of the types of data discussed in this Article along a continuum from "Private" to "Protected." While we may be apt to think of these two terms as synonymous, here I differentiate them in order to distinguish between concepts of ownership and sensitivity or confidentiality. In my construct, the "Privacy" end of the spectrum encompasses data that attracts a social meaning entailing it be treated as confidential—as appropriately known only by the producer and a select few other individuals whom he or she chooses to enlighten. Such data is not only meant to be kept private, it also meant to be market inalienable: for sociocultural reasons, we have decided that it should not be used to make certain market decisions (such as employment-based ones), and thus one incident of its treatment as confidential is the disabling of any such attempted treatment.[152] The "Protected" end of the spectrum, on the other hand, encompasses data that attracts legal protection with regard to its use but may not be similarly treated as inalienable. This type of data includes that which is protected for ownership or exploitation purposes. Unlike "private" data, some of the data falling on this end of the spectrum may garner protection as an incident of *enabling* market dealing by, for instance, allowing only producers to profit from the processing of such data.

As can be seen in the chart, I have graphed the types of data onto the spectrum in the following order: health data occupies the most private position, with medical reputation also falling near it. Self-quantification data, on the other hand, falls right of center toward the protected end,

152. A good example of this is genetic data, protected by the Genetic Information Nondiscrimination Act (GINA), which makes it illegal for employers or health insurers to make decisions based on certain genetic health information. Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233, 122 Stat. 881 (codified in scattered sections of 29, 42 U.S.C. (2012)).

with productivity data falling farther to the right and being deemed the most "protected" of the data types.

Chart 1: Versions of Health-Related Data
on the Spectrum from Private to Protected

This image, designed to chart the intersection between the social meaning of data and the sort of regulation it attracts in the health data space, reflects the following idea: the privacy of a type of data may not track its sensitivity, and the protection offered to a type of data may not reflect its private nature. Consider the way in which health data, the central case as explicated in Part II, is treated as private, while some components of it, when reconfigured into self-quantification data, are more protected than private (say, for instance, self-measured heart rate). This is a result of the variance in social meaning: the former is kept within a bounded social context, while the latter is decontextualized, but accompanied by the normative notion that it is owned by—and thus should be controlled by—the individual that it concerns. Medical reputation data, for its part, involves data that is sensitive in the sense that, as a matter of social meaning, its market exploitation raises eyebrows. While we would not necessarily consider the data point that a person suffers from allergies to be private, we are not comfortable with it being used as the basis to make certain decisions (again, such as employment ones) regarding him or her. From this perspective, self-quantification data need not be private in order to attract protection. Perhaps it attracts protection under an ownership metric; from the standpoint of social meaning, such data *is designed* to be exploited—but only by the person it measures. Thus, it should be protected from exploitation by third parties but need not necessarily be considered particularly sensitive. Finally, productivity data rightly attracts protection, but that protection need not be an incident of its private nature. Indeed, such data may prove difficult to treat as private because it arises in the workplace context. Bringing in the human capital law lens thus offers an alternative language by which to make calls for protection that is not grounded in privacy: it offers a way of reconceptualizing the

social meaning of productivity data unburdened by the baggage of the privacy perspective and responsive to protection concerns that derive from ownership and exploitation metrics. In this way, the human capital law lens expands the slate of available social meanings that can be served by proffered regulatory solutions: protecting our productivity data need *not* mean keeping it private.

B. The Pattern and the Privacy

With its focus on the state of the industry, the human capital law lens may help us to better target the aspects of health-adjacent data in the employment relationship that are actually problematic from a protection perspective.[153] To explain this, it is necessary to examine the nature of productivity data. As explicated in Part III, productivity data measures everything related to the circumstances of knowledge production. The animating idea of the productivity monitoring movement is to uncover the optimal psychological, social, and environmental circumstances for such production, and the actors currently moving in this space use their data to reveal patterns related to peak creativity, innovation, and even happiness. In this way, productivity monitoring is similar to self-quantification, with just one crucial difference: the identity of the party reaping the dividends of collecting and crunching this data. In self-quantification, individuals measure their "autonomic" selves in order to uncover patterns that they can exploit for their own ends;[154] in productivity monitoring, employers harvest information from employees and from the workplace environment to reveal patterns that can be exploited to improve the bottom line—with the financial benefits of applying such insights accruing to the employer. Consider, for instance, the story behind the quote that opened this Article: Hitachi has utilized productivity monitoring to uncover a pattern related to the interaction ingredients for peak happiness in the workplace; it is now deploying its insight in the design of workplace features and culture—but the "formula for happiness . . . remains a trade secret."[155] What constitutes "happiness" is proprietary; workers cannot exploit it for themselves.

The fact that the insights produced by data monitoring and mining in the workplace attract this kind of property protection under the current regulatory regime might explain why the conversation so often returns to

---

153. *See supra* Section IV.A.
154. *See* Moore & Piwek, *supra* note 87, at 311.
155. *See supra* note 1 and accompanying text.

privacy. If the insight generated from the data is always going to accrue to the entity performing the monitoring (here, the employer), then the only way to effect any *protection* for data-producing entities (here, the employees) is to turn to privacy. If one cannot have any protected ownership stake in the actionable insights drawn from one's data, then one needs to prevent the collection of that data in the first place—and that is where privacy comes in. The same is true if one does not have any legal means to obstruct exploitation of the data that is harvested from oneself about the conditions under which one produces knowledge. The modern privacy-in-the-workplace discourse attempts to draw boundaries around the acceptable extent of productivity monitoring. But the introduction of the human capital law lens highlights the complex relationship between individuals and the patterns revealed by the data they produce. While scholars and social commentators in the field[156] have relatively settled on the notion that the raw data one produces is one's own, we are so far unclear on the other aspects of ownership that accompany the propertization of the processing of such data. Lacking a way to conceptualize what it might mean for individuals to share in the ownership of or otherwise have a stake in the insights their data produces, we are continually bounced back to the notion of privacy as a catchall solution. This catchall solution often entirely overlooks the social meaning of the involved data: self-quantification and productivity data is meant to be exploited. It is collected with that end in mind—and this is a concern that privacy protection cannot entirely meet. The application of the human capital law lens, on the other hand, provides a start toward an understanding of such data that conceptualizes it as inalienable and meets the challenge of what I have referred to as "data harvesting" head-on.[157]

Consider that the application of human capital law might encourage us to ask whether certain types of data—like productivity data—should be conceived of as human capital. Professor Lobel, for her part, defines human capital as "the stock of knowledge in all its multiple forms that contributes to productive work, including knowledge that is non-codifiable."[158] Such a definition might well include productivity data, which supports the creation of knowledge that contributes to productive work since it is collected and processed toward the end of optimizing

156. *See supra* Part II.
157. *See supra* Section IV.B.
158. *See* Lobel, *supra* note 129, at 835.

knowledge production. While this would not present an automatic solution—considering the current state of human capital law in the knowledge economy[159]—it could redirect the scholarly and cultural discourse surrounding such data toward ways to generate plausible ownership structures, rather than just treating data as a fundamentally "*a*market" entity capable of keeping its true entity only so long as individuals practice sufficient vigilance in maintaining its confidentiality.

C. The Drive To Quantify: A Slightly Esoteric Concern

The final insight produced by the application of the human capital law lens is a more esoteric one, although not, for that reason, any less important. Consideration of the way in which the productivity monitoring movement attempts to "datafy" knowledge production demonstrates something about the internal logic of Big Data. In essence, Big Data's drive to quantify all human life manifests, in the workplace monitoring space, as an attempt to capture all knowledge, even that "non-codifiable" type of knowledge that our society has traditionally treated as unquantifiable and inextricable from the lives of unique individuals.[160] This drive to "propertize" knowledge production,[161] to make it in essence quantifiable in order to demystify and engineer creativity and innovation, can, when examined in light of human capital law, be read as an attempt to engineer and automate human knowledge. Such automation might, in turn, eliminate human capital. After all, one's ability to produce knowledge may have little value if employers can own, control, and reproduce all of the circumstances necessary to it.

Such an outcome is not, in and of itself, normatively bad. But it is important to notice because it perpetrates a different kind of sociocultural revolution than the one imagined by privacy advocates: the concerns raised by this future scenario are as much epistemological as they are legal or political. As such, they should prompt us to ask questions about the kind of knowledge paradigm we want to live with, and about whether we believe in or desire the sort of utopia promised by Big Data—one where everything is quantified and optimized.[162]

---

159. *See supra* Part IV.

160. *See* Lobel, *supra* note 129, at 835.

161. *See id.* at 840-43.

162. *See* Frischmann & Selinger, *supra* note 84, at 373 (The authors of this article delineate three different "utopias" that characterize the current technological landscape: the Cosean Utopia of Frictionless Transactions and Perfectly Efficient Market Exchange; the Taylorist Utopia of Scientifically Managed Human Labor and Perfectly Productive Workplaces;

VI. CONCLUSION

The health and health-adjacent data conversation is currently dominated by the privacy perspective. This is so despite the fact that the ecosystem for such data has evolved beyond the bounds of the central case of health data. Scholars grappling with the expansion of this datasphere—especially when it intersects with the employment relationship—have been heretofore overly wedded to the privacy perspective, apt to frame all of their concerns with the decontextualization and increasingly free flow of health-type information as concerns about privacy, and to make repeated, tired recommendations for regulatory intervention that simply enlarges current confidentiality provisions like HIPAA.[163] This Article has attempted to counter such a trend by offering human capital law as a lens for considering health data beyond privacy. By sketching the current ecosystem, carving out the existence within it of a new category of productivity data, and then subjecting this category to analysis from the perspective of human capital law, this Article illuminated a variety of different concerns surrounding such data, and introduced an alternative analytical framework from which to offer interventions. If we hope to truly understand the ways in which Big Data is transforming our workplaces—and, ultimately, our lives—we need to strengthen our capacity for both discerning the meanings of different types of data and effectively regulating their use. I hope for the human capital law lens to be a step in this direction.

---

and the Nozickian Experience Machine Utopia of Technologically Managed Experience and Perfectly Happy Lives.).

163. *See supra* Part II.