2021

The Law of Employee Data: Privacy, Property, Governance

Matthew T. Bodie

SAINT LOUIS UNIVERSITY SCHOOL OF LAW
Legal Studies Research Paper Series

No. 2021-14

The Law of Employee Data: Privacy, Property, Governance

Matthew T. Bodie
Saint Louis University School of Law

Indiana Law Journal, Vol. 97, 2021-2022

THE LAW OF EMPLOYEE DATA: PRIVACY, PROPERTY, GOVERNANCE

Matthew T. Bodie*

ABSTRACT

The availability of data related to the employment relationship has ballooned into an unruly mass of personal characteristics, performance metrics, biometric recordings, and creative output. The law governing this collection of information has been awkwardly split between privacy regulations and intellectual property rights, with employees generally losing on both ends. This Article rejects a binary approach that either carves out private spaces ineffectually or renders data into isolated pieces of ownership. Instead, the law should implement a hybrid system that provides workers with continuing input and control without blocking efforts at joint production. In addition, employers should have fiduciary responsibilities in managing employee data, and workers should have collective governance rights over the data's collection and use.

* Callis Family Professor and Co-Director, Wefel Center for Employment Law, Saint Louis University School of Law. Many thanks to participants at: the Privacy Law Scholars Conference, especially to Gaia Bernstein as commentator and to Lilian Edwards, Leslie Francis, Pauline Kim, Matthew Kugler, and Elana Zeide for their comments; the Colloquium on Scholarship in Employment and Labor Law, including co-panelists Veena Dubal, Charlotte Garden, and JoAnne Sweeney; and the Boston College Law School's Markets and Regulation Workshop, especially hosts Natalya Shnitser, Shu-Yi Oei, and Diane Ring. Thanks as well to Catherine Fisk for her comments. I am much obliged for research assistance from Danielle Durban, Andrew Keady, and Michael McMahon.

TABLE OF CONTENTS

INTRODUCTION 2
I. DATA IN THE EMPLOYMENT RELATIONSHIP 7
II. REGULATION OF EMPLOYEE DATA 15
A. Employee Privacy Protections 15
B. Property Rights in Employee Data 25
III. FAILING PARADIGMS IN THE REGULATION OF EMPLOYEE DATA 33
A. The Divide between Personal and Business-Related 33
B. The Embeddedness of the Worker within the Economic Firm 39
C. The Digital Divide: Platform Drivers and Professional Athletes 45
IV. A NEW REGIME FOR EMPLOYEE DATA: PRIVACY, PROPERTY, AND GOVERNANCE 51
A. A Hybrid Approach to the Privacy/Property Conundrum 52
B. Employers as Information Fiduciaries 58
C. Worker Participation in Informational Governance 62
CONCLUSION 67

INTRODUCTION

The Enron Corpus is a collection of 1.6 million emails, calendar entries, and notes that were made publicly available in 2003 by the Federal Energy Resource Commission (FERC).[1] Over 600,000 emails within the Corpus were sent or received by 158 Enron executives through their employer's Microsoft Outlook database.[2] FERC seized the database are part of its investigation of illegal Enron manipulation of the energy markets—one lesser-known slice of the company's wide-ranging malfeasance. At the conclusion of the investigation, the Commission released the database to the public to substantiate its findings.[3] In its original state, the Corpus was an

[1] Rebecca Bolin, *Risky Mail: Concerns in Confidential Attorney-Client Email*, 81 U. CIN. L. REV. 601, 648 (2012).

[2] *Id.*; *see also* Corinne Purtill, *The Emails that Brought Down Enron Still Shape Our Daily Lives*, QUARTZ.COM, Feb. 19, 2019, https://qz.com/work/1546565/the-emails-that-brought-down-enron-still-shape-our-daily-lives/.

[3] Nathan Heller, *What the Enron E-Mails Say About* Us, NEW YORKER, July 17, 2017, https://www.newyorker.com/magazine/2017/07/24/what-the-enron-e-mails-say-about-us.

amorphous set of unwieldy and unusable data. However, an MIT researcher worked to collect, manage, and rerelease the data in a format that researchers found to be eminently usable.[4] The dataset has since become fodder for over 100 research projects and commercial applications in computer science.[5] It has been most influential, however, as a training ground for artificial intelligence. Using these emails as raw data for real conversations, AI systems from Apple's Siri to Google's "smart compose" feature developed their understanding of human speech based on this set of communications amongst Enron employees.[6]

The story of the Enron Corpus raises many concerns. It's disturbing to hear that AI systems learned about human interaction by churning through frenzied missives from workers at a company whose operations were going up in smoke.[7] Enron has become synonymous with scandal, subterfuge, and excess—and yet these emails and calendar posts are teaching our algorithms how to think. Enron executives were not representative of the populace as a whole, in myriad ways, and still their flawed culture was embedded in machine learning systems.[8] The use of the Corpus represents another example of AI systems learning from flawed and biased examples to reproduce inequality.[9]

---

[4] Purtill, *supra* note 2.

[5] Heller, *supra* note 3; Purtill, *supra* note 2.

[6] Jessica Leber, *The Immortal Life of the Enron E-Mails*, MIT TECH. REV. , July 2, 2013, https://www.technologyreview.com/2013/07/02/177506/the-immortal-life-of-the-enron-e-mails/.

[7] Purtill, *supra* note 2 ("While the emails offer compelling evidence of how people talk to each other, specifically, they offer evidence of how people who thrived at a morally compromised US corporation in the late 1990s and early 2000s talked to each other.").

[8] Amanda Levendowski, *How Copyright Law Can Fix Artificial Intelligence's Implicit Bias Problem*, 93 WASH. L. REV. 579, 611 (2018) ("If you think there might be significant biases embedded in emails sent among employees of Texas oil-and-gas company that collapsed under federal investigation for fraud stemming from systemic, institutionalized unethical culture, you would be right.").

[9] Ifeoma Ajunwa, *The Paradox of Automation As Anti-Bias Intervention*, 41 CARDOZO L. REV. 1671, 1673 (2020) (discussing how algorithms may "serve to reproduce inequalities at scale"); Jeffrey Dastin, *Amazon Scraps Secret AI Recruiting*

The release of the Enron Corpus into the public domain also violated these employees' personal privacy. The original dump included the emails without any redactions, leaving in phone numbers, Social Security numbers, bank records, and other tools for identity theft.[10] Personal details came abruptly to light, such as complaints from the CEO's daughter about weddings and even a heretofore undiscovered office tryst.[11] The dataset was redacted on several occasions to protect personal information, but even mundane emails inevitably exposed the authors to unexpected scrutiny.[12] These discussions of job performance, workplace gossip, and day-to-day grumbles and tribulations—along with allegations of deeply unethical behavior—were inextricably intertwined with the employees who wrote them.

There is yet another, mostly neglected aspect of the Enron Corpus: our new frontier in the creation of value. The dataset has been used over and over again by researchers to develop incredibly rich advancements in artificial intelligence. Simply by going about their daily business within the company, Enron employees developed an interconnected web of interactions providing raw material for cutting-edge research. In theory, this type of data now can be found at thousands of companies that provide email, texting, Slack channels, G-Chat, Zoom meetings, and other instances of recorded human conversation. But this data is not publicly available. The Enron data is thus something of a unicorn—a set of real business interactions that were made available to all and do not have meaningful copyright, privacy, or trade secret protections that might entangle researchers in legal claims.[13] The

---

Tool that Showed Bias against Women, REUTERS (Oct. 10, 2018 6:04 P.M.) (discussion Amazon recruiting algorithm that preferred men named Jared who played lacrosse).

[10] Bolin, *supra* note 1, at 648.

[11] *Id.*; Leber, *supra* note 6.

[12] Leber, *supra* note 6.

[13] Levendowski, *supra* note 8, at 610-11 (describing the Enron emails as akin to "orphan works" and noting that "the Enron emails are perceived as posing an infinitesimally low legal risk because, though some of the Enron emails are protectable under copyright law, the practical likelihood of former Enron employees suing for copyright infringement is exceedingly remote"); Leber, *supra* note 6 ("A research ecosystem still blooms around the corpus because there is nothing else like it in the public domain. If it didn't exist, research into business e-mails could be done only by people with access to big corporate or government servers.")

former employees and their company have been completely cut off from any claims of ownership, confidentiality, or protection over their work.

The new ecosystem of Big Data and machine learning has transmogrified ordinary interactions into valuable fuel. Information is vacuumed off of individuals in the course of their daily lives and used to provide new products, better services, and tailored advertising—"surveillance capitalism."[14] To date, the legal and policy discussions around information privacy and data protection have largely focused on our roles as consumers and the conduct of our private lives.[15] Data in and from employment—our worklife data—has been neglected.

We generally regulate worker data[16] under two legal categories: privacy and intellectual property. Privacy laws are invoked to shield workers' personal information in specific contexts, such as lockers, drug tests, genetic information, and credit scores. Intellectual property generally hands employment-related data over to the employer through legal mechanisms such as trade secrets or "work-for-hire." This sharp divide between personal and employment-related information is meant to protect workers' autonomy while enabling them to participate in team production. This divide is breaking down, however, as employers realize the value of personal information to the workplace, and workers find their identities wrapped up in their vocations. The SARS-Cov-2 pandemic has only exacerbated this collapse, as employers take employees' temperatures, trace their contacts on and off

[14] SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM (2019).

[15] Sam Adler-Bell & Michelle Miller, *The Datafication of Employment*, CENTURY FOUNDATION (Dec. 19, 2018), https://tcf.org/content/report/datafication-employment-surveillance-capitalism-shaping-workers-futures-without-knowledge/?agreed=1 ("For consumers, the digital age presents a devil's bargain . . . . But less well understood is the way data—its collection, aggregation, and use—is changing the balance of power in the workplace.").

[16] This Article uses "employee data," "worker data," and "worklife data" interchangeably. Additionally, I will sometimes use "employee" to include workers that may not be considered employees under certain legal definitions. Likewise, the term "employer" will similarly apply to firms that hire people to provide labor, even when that is outside of a particular legal framework. When the legal definition of "employee" or "employer" is relevant to the Article, I will note it.

the job, and monitor those who are working from home.[17] The divide cannot hold. Workers are finding themselves virtually enmeshed within their businesses—without control, ownership, or regulation.

In response to this increasingly fraught set of dynamics, advocates and academics have generally proposed a ratcheting-up of workplace privacy protections.[18] This Article takes a broader view, looking at a spectrum of potential legal mechanisms that can protect, secure, and reengage employees in their relationship with their data. Rather than dwelling on the personal nature of specific data or the expectation of privacy within a location, the employee should be empowered with respect to her data across a variety of contexts. That empowerment is founded on concepts of privacy, intellectual property, and governance to strengthen the bonds between the worker and her data. This multidimensional approach is necessary to manage the myriad aspects of the employment relationship. Moreover, it is emblematic of the success enjoyed by workers who are in relative positions of power and can best exploit the legal regime to protect their interests.

In order to situate our understanding, Part I of the article reviews the use of data in the employment relationship. Companies have always collected and analyzed information about their workers, but the types of data, methods of extraction, and analytics of use have dramatically changed over time. Part II surveys the existing legal regulation of employee data within the United States. Part III examines complications of individual employee data within the concept of the firm. In particular, I discuss the merging of the categories of personal data and business-related data, as well as the embeddedness of

---

[17] *See, e.g.,* Matthew T. Bodie & Michael McMahon, *Employee Testing, Tracing, and Disclosure as a Response to the Coronavirus Pandemic*, 64 WASH U. J.L & POL'Y (forthcoming 2021); Mohana Ravindranath, *Coronavirus Opens Door to Company Surveillance of Workers,* POLITICO (June 26, 2020, 4:30 a.m.), https://www.politico.com/news/2020/06/26/workplace-apps-tracking-coronavirus-could-test-privacy-boundaries-340525.

[18] *See, e.g.*, Ifeoma Ajunwa, Kate Crawford & Jason Schultz, *Limitless Worker Surveillance*, 105 CAL. L. REV. 735, 772-76 (2017) (describing potential reforms in employee privacy protections); Sissi Cao, *Amazon Unveils AI Worker Monitoring for Social Distancing, Worrying Privacy Advocates,* OBSERVER (June 16, 2020, 12:11 p.m.), https://observer.com/2020/06/amazon-artificial-intelligence-monitor-warehouse-worker-social-distancing-coronavirus/.

employees within the economic firm. The Article then compares the data relationship that firms have with less empowered workers, such as platform drivers, with empowered workers—specifically, professional athletes. Finally, in Part IV the Article proposes a new framework for regulating worker data: outfitting employees with continuing privacy and property rights over their data; imposing fiduciary responsibilities on the employer as to this data; and providing workers with participation rights in the governance of their firms.

I. DATA IN EMPLOYMENT: PAST AND PRESENT

As a preliminary matter, I should note that this article takes a very expansive view of data in employment. It includes any information that concerns the employee or the work done by the employee. It is information generated by the employee. Sometimes that information is seen as distinctly personal, as in the employee's weight, temperature, or political leanings, but it is also information that the employee generates within the scope of employment, as in the calls that the salesperson makes to customers, the path of employee movements tracked by GPS, and gossip exchanged between coworkers.[19] This expansive view is necessary to capture the breadth of interaction between employee and employer, and the overwhelming amount of data that is available to collect and use. The key distinction is that the data involves a particular person—an individual employee—but is not confined to "personal" information.[20]

---

[19] The data need not be generated intentionally; it can be a byproduct of their actions or words. *See, e.g.*, Jefferson Graham & Laura Schulte, *Wisconsin Workers Embedded with Microchips*, USA TODAY Aug. 1, 2017, https://www.usatoday.com/story/tech/talkingtech/2017/08/01/wisconsin-employees-got-embedded-chips/529198001/.

[20] The definitional questions around data protection likely deserve more interrogation, but by choosing a broad scope I hope to take a detour around them. *See, e.g.*, Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and A New Concept of Personally Identifiable Information,* 86 N.Y.U. L. REV. 1814 (2011).

Collecting and using data about workers is endemic to the employment relationship throughout its history.[21] The question has been the nature and scope of the information exchange. Frederick Taylor based his system of scientific management on direct observation of workers in the process of working.[22] Taylor focused on the nuts and bolts of the actions undertaken, and he largely believed that workers were interchangeable parts. It took the development of the field of personnel management to recognize the importance of the individual to the production process.[23] But this change also meant an expansion of the relevant zone of information—an expansion to include the worker's personality and desires.[24] Henry Ford, an early practitioner of personnel management, created a "Sociological Department"

---

[21] *See, e.g.*:, Ajunwa, Crawford & Schultz, *supra* note 18, at 737 ("Ubiquitous employer surveillance of workers has a long and rich history as a defining characteristic of workplace power dynamics, including the de facto abrogation of almost any substantive legal restraints on its use."); Ethan S. Bernstein, *Making Transparency Transparent: The Evolution of Observation in Management Theory*, 11 ACAD. MGMT. ANNALS 217, 218 (2016) ("Observation has always been a foundational element of management and, indeed, of daily life. Only through observation can individuals and organizations understand and control their conditions.").

[22] Calvin Morrill & Danielle S. Rudes, *Conflict Resolution in Organizations*, 6 ANN. REV. L. & SOC. SCI. 627, 629 (2010) ("Frederick Taylor developed the best-known engineering approach in scientific management, which operated from the premise that direct observation of work practices could provide the basis for optimal job design and worker productivity."); *see also* Frederick Taylor, *A Piece Rate System, Being a Step toward Partial Solution of the Labor Problem*, 16 TRANSACTIONS 856 (1895). Taylor was perhaps the most prominent member of the "systematic management" movement between 1880 and 1920. Sanford M. Jacoby, *A Century of Human Resources Management*, *in* INDUSTRIAL RELATIONS TO HUMAN RESOURCES AND BEYOND 147, 148 (Bruce E. Kaufman et al. eds., 2003).

[23] BRUCE E. KAUFMAN, THE ORIGINS & EVOLUTION OF THE FIELD OF INDUSTRIAL RELATIONS IN THE UNITED STATES 24 (1993); *see also* GORDON S. WATKINS, AN INTRODUCTION TO THE STUDY OF LABOR PROBLEMS 476-77 (1922) ("The old scientific management failed because it was not founded upon a full appreciation of the importance of the human factor. It was left to the new science of personnel management to discover and evaluate the human elements in production and distribution.").

[24] KAUFMAN, *supra* note 23, at 24.

to delve into the workers' personal lives.[25] The Department deployed a team of 150 to investigate the lifestyle of each Ford employee and their personal habits, such as smoking, drinking, and gambling, as well as their spending and saving habits.[26] As it developed as a field of study, personnel management (later called human resources management) grew to include the use of psychological tests,[27] organizational dynamics,[28] and even the effects of monitoring itself.[29]

The last 20 years have seen a dramatic leap forward in the ability to collect and use massive sets of quantitative data. Colloquially known as "Big Data," the combination of data and new tools to crunch the data has unlocked new insights about human behavior, revolutionizing the field of advertising and dramatically reshaping our consumer relationships.[30] And its influence extends to all corners of our lives, from dating apps to traffic-displaying maps to recommended prison sentences.[31] Big Data in the employment relationship—sometimes referred to as "people analytics"—has created a new

---

[25] Samuel M. Levin, *Ford Profit Sharing, 1914-1920: I. The Growth of the Plan*, *in* HENRY FORD: CRITICAL EVALUATIONS IN BUSINESS AND MANAGEMENT 160, 163 (John C. Wood & Michael C. Wood eds., 2003) (noting that the Sociological Department's investigations would "examine home conditions, to find out whether a man drinks, how he spends his evenings, whether he has a bank account, dependents, etc.").

[26] M. Todd Henderson, *The Nanny Corporation*, 76 U. CHI. L. REV. 1517, 1541 (2009) (footnotes omitted). Ford later disbanded the Sociological Department and stated: "Welfare work that consists in prying into employees' private concerns is out of date." HENRY FORD, MY LIFE AND WORK 130 (1922).

[27] Maureen E. Mulvihill, Karraker v. Rent-A-Center: *Testing the Limits of the ADA, Personality Tests, and Employer Preemployment Screening*, 37 LOY. U. CHI. L.J. 865, 873 (2006).

[28] Wickham Skinner, *Managing Human Resources*, HARV. BUS. REV., Sept. 1981.

[29] *See* Fritz J. Roethlisberger, *The Hawthorne Experiments*, *in* CLASSICS OF PERSONNEL MANAGEMENT 16, 16-17 (Thomas H. Patten, Jr. ed., 1979).

[30] ZUBOFF, *supra* note 14, at 138-55 (discussing the "dispossession" cycle of consumer data).

[31] *See* FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION (2015) (describing examples).

data-driven approach to human resources management.[32] One early example was popularized in the book and film *Moneyball*, which described how the general manager of baseball's Oakland Athletics relied on quantitative data analysis rather than anecdotal scouting reports.[33] The team's methods in *Moneyball* seem downright rudimentary when compared with the sophisticated techniques in use today.[34]

The "people analytics" methodology can generally be broken down into two steps: (1) collecting pools of quantitative data from employees, and (2) analyzing the data to make workplace decisions.[35] Technological advances have enabled employers to survey a vastly broader set of questions and answers using information from and about employees. The development and widespread use of the Internet, email, text messaging, and other recorded methods of interaction have made the collection of communication relatively costless for employers, going all the way back to the late 1990s.[36] Video and audio recording are now done digitally, making them much easier to record and store.[37] Other electronic devices record employee movement, browser history, heart rate, temperature, and interactions with other employees.[38] One people-analytics invention, known as a "Sociometric Badge," incorporates a

---

[32] Don Peck, *They're Watching You at Work,* ATLANTIC, Dec. 2013, at 72, *available at* http://www.theatlantic.com/magazine/archive/2013/12/theyre-watching-you-at-work/354681/. *See generally* Matthew T. Bodie, Miriam A. Cherry, Marcia L. McCormick & Jintong Tang, *The Law and Policy of People Analytics*, 88 U. COLO. L. REV. 961, 964-73 (2017).

[33] MICHAEL LEWIS, MONEYBALL: THE ART OF WINNING AN UNFAIR GAME (2003).

[34] *See, e.g.*:, Josh Bersin, *The Geeks Arrive in HR: People Analytics Is Here*, FORBES (Feb. 1, 2015), http://www.forbes.com/sites/joshbersin/2015/02/01/geeks-arrive-in-hr-people-analytics-is-here/ (discussing a people analytics meeting involving "eight PhD statisticians, engineers, and computer scientists together, all working on people analytics for their companies").

[35] Bodie, Cherry, McCormick & Tang, *supra* note 32, at 973.

[36] *See, e.g.*:, Lisa Guernsey, *The Web: New Ticket to a Pink Slip*, N.Y. TIMES, Dec. 16, 1999, at G1 ("In 1999, at least 45 percent of employers said they monitored their employees' phone calls, computer files or email messages, according to the American Management Association.").

[37] Ajunwa, Crawford & Schultz, *supra* note 18, at 738.

[38] *Id.* at 743.

microphone, an infra-red device, and a motion detector to measure aspects of human interactions.[39] Employers can use the data from the badge to determine when employees are interacting, where, for how long, and with what level of emotional valence (based on sound data).[40]

To match up with this massive influx of data, automated decision systems—also known as algorithms, data analytics, machine learning, and artificial intelligence—are now much more sophisticated at crunching this data and providing novel insights. Rather than needing a specific hypothesis to test on the data, these new analytics tools can work through the numbers to find unexpected correlations.[41] As one example, Google applies its own brand of data analytics to its human resources department, which it calls "People Operations."[42] The company prides itself on taking HR decisions out of the hands of individual managers and instead giving them to groups.[43] These decisionmakers are then given data and data-crunching algorithms to better manage their methods. Among the unusual approaches that Google has taken: paying talented workers much more than average workers in a particular job; shrinking plate sizes in the corporate cafeteria to reduce caloric intake; and adding perks like ATMs, microkitchens, and onsite laundry machines to help workers balance their professional and personal lives.[44] For its "Project Aristotle," an internal initiative to study the metrics of success between Google teams, the company collected data along a myriad of lines to determine what components created a top team.[45]

---

[39] BEN WABER, PEOPLE ANALYTICS 14-16 (2013).

[40] *Id.* at 179-81.

[41] *See* Matthew T. Bodie, *Workplace Freakonomics*, 14 I/S: J.L. & POL'Y FOR INFO. SOC'Y 37, 38 (2017) (describing "freakonomics analytics" as those tools looking for "unusual, surprising, and counterintuitive correlations between various behaviors and phenomena that can only now be understood--or, at least, seen--through data analytics").

[42] Adam Bryant, *Quest to Build a Better Boss*, N.Y. TIMES, Mar. 12, 2011, at BU1 (noting that "'people operations' . . . is Googlespeak for human resources").

[43] LASZLO BOCK, WORK RULES! 12 (2015).

[44] *Id.*

[45] Charles Duhigg, *Group Study: What Google Learned From Its Quest to Build the Perfect Team*, N.Y. TIMES, Magazine, at 20, 26 (Feb. 28, 2016) (finding that teams thrived most when they engendered a sense of psychological safety).

Much of the data collected in this new environment could be considered personal—patterns of speech, laundry habits, and preferences for psychological safety. The line between person as individual and person as employee has become significantly blurred.[46] The SARS-CoV-2 pandemic has only exacerbated this trend. Long considered to be particularly private information, employee health data has been thrust into the forefront as newly relevant to workplace operations.[47] Employers are taking their workers' temperatures, administering novel coronavirus tests, and managing the news of an employee's positive test with other workers and medical professionals.[48] Many employers are considering the use of contact tracing to determine who has come in contact with employees who catch the virus.[49] Workers must wear masks and self-quarantine, and may be required to vaccinate.[50]

---

[46] Ajunwa, Crawford & Schultz, *supra* note 18, at 738-39 ("What is novel, and of real concern to privacy law, is that rapid technological advancements and diminishing costs now mean employee surveillance occurs both inside and outside the workplace—bleeding into the private lives of employees."); Leora Eisenstadt, *Data Analytics and the Erosion of the Work/Nonwork Divide*, 56 AM. BUS. L.J. 445, 448 (2019) ("[T]he explosion of technological advances that allow employers to monitor and rely upon workers' off-duty conduct will likely weaken the dividing line between work and nonwork in dramatically greater and more troubling ways than ever before.")

[47] Russell Brandom, *Workers from Amazon, Instacart, and Others Are Calling in Sick to Protest Poor Virus Protections*, VERGE, May 1, 2020, https://www.theverge.com/2020/5/1/21243905/mayday-strike-boycott-amazon-target-walmart-whole-foods-instacart-shiptstrike; Jill Colvin, *Trump Order Keeps Meatpacking Plants Open, But Unions Say Workers Unsafe,* CHI. TRIB., April 29, 2020, https://www.chicagotribune.com/coronavirus/ct-nw-coronavirus-trump-slaughterhouse-meatpacking-20200429-34sj5c3neray7jrylc7l3pnnfm-story.html; Adam Jeffery, *Healthcare Workers Protest for Vital Protection Equipment*, CNBC.COM, APRIL 20, 2020, https://www.cnbc.com/2020/04/18/healthcare-workers-protest-for-vital-protection-equipment.html;

[48] Bodie & McMahon, *supra* note 17.

[49] Ravindranath, *supra* note 17 ("Employers are rushing to use digital tracking technology to reduce virus transmission in the workplace.").

[50] Zlati Meyer, *Can You Get Fired If You Don't Get a COVID-19 Vaccine? Yes*, FAST COMPANY, FEB. 19, 2021, https://www.fastcompany.com/90605815/can-you-get-fired-if-you-dont-get-a-covid-vaccine-yes.

Technology has also brought home and personal life into the workplace. Consider: the doctor who drunkenly assaulted an Uber driver; a CEO's financial donation in support of California's Proposition 8; a daycare worker's Facebook post that she hates being around kids.[51] In these cases, what employees considered to be private ended up becoming very public and ultimately affected the reputation of their employers. Information about one employee can change the valuation of a company, the arc of its business model, the sheen of its brand. This is obviously true when it comes to corporate leaders, as examples such as Steve Jobs, Martha Stewart, and Kylie Jenner illustrate.[52] But even frontline workers can have an impact on the reputation of the company.[53] In service-oriented businesses, the work of individual employees is the key to building the value of the brand.[54] Reputation scores are available on dozens of websites, and social media can hold a vast mélange of observations and complaints about individual customer interactions, making employees more important than ever to brand and business value.[55] And information about what they do in their off time now has much broader ramifications.

---

[51] Matthew Bodie, *The Internet Wants You to Lose Your Job*, QUARTZ.COM (Feb. 3, 2016), https://qz.com/608697/the-internet-wants-you-to-lose-your-job/ (noting that employee misfires on social media affect brand reputation).

[52] Tom C. W. Lin, *Undressing the CEO: Disclosing Private, Material Matters of Public Company Executives*, 11 U. PA. J. BUS. L. 383, 384 (2009).

[53] One drugstore-chain cashier was so warm and friendly with customers that a nationally syndicated talk show singled him out for praise. Joe Holleman, *Local Walgreens Cashier Surprised in Store by Ellen DeGeneres*, ST. LOUIS POST-DISPATCH (Jan. 4, 2018), https://www.stltoday.com/news/local/columns/joe-holleman/local-walgreens-cashier-surprised-in-store-by-ellen-degeneres/article_b73acb94-2058-53e2-820d-a21ca5e241e7.html.

[54] *See, e.g.*:, TONY HSIEH, DELIVERING HAPPINESS: A PATH TO PROFITS, PASSION, AND PURPOSE (2010).

[55] Marie-Cécile Cervellon & Pamela Lirio, *When Employees Don't 'Like' Their Employers on Social Media*, MIT SLOAN MGMT. REV., Feb. 2017, https://sloanreview.mit.edu/wp-content/uploads/2016/11/f11dc7eeaa-3.pdf.

In a growing number of employment relationships, employee-generated data constitutes, in whole or in part, the output of the employer.[56] To take but a few examples: doctors give medical advice and prescribe medicine; lawyers provide legal counsel and advocacy; comedians perform live or on a recorded medium. We understand this more intuitively when it comes to formal intellectual property: copyrights become the property of the firm through the "work-for-hire" doctrine, while most employee patents are assigned to the company as part of the employment agreement.[57] But slippery sets of information have been enfolded into trade secret law, covering employee-created information such as client lists, marketing plans, business strategies—literally any information that has inherent economic value because it is not generally known or readily ascertainable by others, and which is kept private.[58] In an era of Big Data, algorithms have become heavily guarded secrets, including not only their methods but also the data used to drive them.[59] And that data is often provided by employees. Uber and Lyft, for example, track their employees as part of a huge algorithm of traffic and transportation that has significant value on its own.[60] There is even evidence that some companies may be profiting from their employees' data through sales to third parties.[61] After all, the Enron Corpus was not only the day-to-day communication between individual employees; it was also a valuable dataset of human interaction with its own independent value.

The upshot is this: employment now means handing over even more of our individual selves, in the form of data, in service to a communal

---

[56] *See* JEREMIAS PRASSL, HUMANS AS A SERVICE: THE PROMISE AND PERILS OF WORK IN THE GIG ECONOMY (2018).

[57] *See* Part II.B *infra*.

[58] UNIFORM TRADE SECRETS ACT § 1(4) (amended 1985), 14 U.L.A. 529 (2005).

[59] Sonia K. Katyal, *Private Accountability in the Age of Artificial Intelligence*, 66 UCLA L. REV. 54, 123–24 (2019).

[60] Tom Simonite, *When Your Boss is an Uber Algorithm*, MIT TECH. REV., Dec. 1, 2015, https://www.technologyreview.com/2015/12/01/247388/when-your-boss-is-an-uber-algorithm/.

[61] Adler-Bell & Miller, *supra* note 15 (discussing how corporate employee surveillance enables "a pernicious form of rent-seeking—in which companies generate huge profits by packaging and selling worker data in marketplace[s] hidden from workers' eyes").

enterprise. Nothing seems to be off the table. In this world of employee embeddedness within an immersive world of data, how will law react to its construction of the employment relationship? Before answering this question, we first review the legal environment for worker data at present.

II. REGULATION OF EMPLOYEE DATA

Employers must abide by a variety of different statutory, regulatory, and common-law schemes when they are collecting and using employee data. These schemes can be grouped into two rough categories: privacy protections for employees and their data, and the assignment of property rights as to employee data. Privacy law serves to protect information by punishing those who collect, use, or disclose the information without legal authorization or justification. Property law, on the other hand, protects information by giving the owner a bundle of potential rights over the use of the property.[62] These two different legal regimes do not apply to the same sets of employee data, but together they create the topography from which employees and employers operate.[63]

A. Employee Privacy Protections

[62] *See* Henry E. Smith, *Exclusion and Property Rules in the Law of Nuisance*, 90 VA. L. REV. 965, 967 (2004) (noting that Coase saw property as "a collection of use rights, the so-called 'bundle of sticks'").

[63] For a discussion of the different ramifications between liability rules and property rules, see Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089, 1115-17 (1972); *see also* Lucian Arye Bebchuk, *Property Rights and Liability Rules: The Ex Ante View of the Cathedral*, 100 MICH. L. REV. 601 (2001); Richard R.W. Brooks, *The Relative Burden of Determining Property Rules and Liability Rules: Broken Elevators in the Cathedral*, 97 NW. U. L. REV. 267, 291-92 (2002); Louis Kaplow & Steven Shavell, *Property Rules Versus Liability Rules: An Economic Analysis*, 109 HARV. L. REV. 713, 715 (1996).

No comprehensive U.S. privacy law protects employee's information; rather, we have a loose network of provisions.[64] The broadest set of protections comes from constitutional law and the common law. The U.S. Constitution prohibits unreasonable searches and seizures under the Fourth Amendment[65] and potentially extends a federal right of information privacy,[66] but these protections only apply to public-sector employees.[67] California's constitutional protections for privacy do protect both public- and private-sector employees;[68] the California Supreme Court has analogized these protections to the privacy tort of intrusion upon seclusion recognized in American common law.[69] The intrusion tort imposes liability when one has invaded "the solitude or seclusion of another or [their] private affairs or concerns" if the intrusion is "highly offensive to a reasonable person."[70]

---

[64] Alan F. Westin, *Privacy in the Workplace: How Well Does American Law Reflect American Values?*, 72 CHI.-KENT L. REV. 271, 282–83 (1996) ("[T]he U.S. approach to privacy remains a more eclectic blend of constitutional interpretation, pin-pointed and sector-specific legislation, sector-based administrative agency rules, common-law judicial interpretation, labor-management bargaining (where employees are union-represented), voluntary organizational policies, and market-based dynamics."). For a comparative look, see Arianne Renan Barzilay, *Data Analytics at Work: A View from Israel on Employee Privacy and Equality in the Age of Data-Driven Employment Management*, 40 COMP. LAB. L. & POL'Y J. 421, 422 (2019).

[65]. *See, e.g.*, O'Connor v. Ortega, 480 U.S. 709, 725-26 (1987); City of Ontario v. Quon, 560 U.S. 746, 756-57 (2010).

[66] Nat'l Aeronautics & Space Admin. v. Nelson, 562 U.S. 134, 138 (2011) (assuming, without deciding, that government workers had a right to information privacy).

[67] *Cf.* Pauline T. Kim, *Privacy Rights, Public Policy, and the Employment Relationship*, 57 OHIO ST. L.J. 671, 674 n.17 (1996) ("In rare cases, where a private employer is acting as an instrument or agent of the government, constitutional privacy protections may extend to workers in the private sector.").

[68] CAL. CONST. art. I, § 1 (providing for "inalienable rights" including "pursuing and obtaining safety, happiness, and privacy"); Hill v. Nat'l Collegiate Athletic Ass'n, 865 P.2d 633 (Cal. 1994) (holding that held that the state's constitutional right of privacy extended to private actors, including private-sector employers).

[69] Hernandez v. Hillsides, Inc., 211 P.3d 1063, 1073 (Cal. 2009) ("The right to privacy in the California Constitution sets standards similar to the common law tort of intrusion.").

[70] RESTATEMENT (SECOND) OF TORTS § 652B (AM. LAW INST. 1977).

Courts have found liability in a variety of workplace situations, such as when an employer spied on an employee to get information for a workers' compensation claim,[71] when "fake" employees were dispersed into the workforce to get private information about fellow workers,[72] when lockers were searched without consent,[73] and when cameras were installed in bathrooms or private offices.[74] The *Restatement of Employment Law* has redefined the tort in the employment context to protect the physical person and physical and electronic locations[75] as well as personal information.[76] In addition, the Restatement prohibits the disclosure of information that was confidentially provided to the employer, in a manner similar to the tort of public disclosure of private fact.[77]

Beyond these constitutional and common-law protections are a collection of statutory and regulatory provisions that have at least a glancing relationship to employee data. But this collection is incomplete. As to personal data about an employee's health, for example, the common law tort does provide some protection against collection and intrusion in extreme cases.[78] But there is no federal or state law generally protecting the privacy of employee health information. Many believe the federal Health Information Portability and Accountability Act (HIPAA)[79] applies to protect such data, but

---

[71] *See, e.g.*:, York v. General Electric Co., 759 N.E.2d 865 (Ohio Ct. App. 2001).

[72] *See, e.g.*:, Johnson v. K-Mart Corp., 723 N.E.2d 1192 (Ill. App. Ct. 2000).

[73] *See, e.g.*:, K-Mart Corp. Store No. 7441 v. Trotti, 677 S.W.2d 632 (Tex. App. 1984).

[74] *See, e.g.*:, Elmore v. Atlantic Zayre, Inc., 341 S.E.2d 905, 906-907 (Ga. Ct. App. 1986) (bathroom); Hernandez v. Hillsides, Inc., 211 P.3d 1063, 1073 (Cal. 2009) (office).

[75] RESTATEMENT OF EMPLOYMENT LAW § 7.03 (AM. LAW INST. 2015).

[76] *Id.* § 7.04.

[77] *Compare id.* § 7.05 *with* RESTATEMENT (SECOND) OF TORTS § 652D (AM. LAW INST. 1977).

[78] Miller v. Motorola, Inc., 560 N.E.2d 900 (Ill. App. Ct. 1990) (employer disclosure of employee's mastectomy). *But see* Feminist Women's Health Center v. Superior Court of Sacramento Co., 61 Cal. Rptr. 2d 187, 195 (Cal. App. 3d 1997) (finding that a requirement that employees demonstrate self-cervical exams was not a privacy intrusion because of the employer's "fundamental goal of educating women about the function and health of their reproductive systems").

[79] Health Information Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 26, 29, and 42 U.S.C.).

HIPAA only covers health plans, health care providers, and health care clearinghouses.[80] Employers are not covered unless they provide health care or self-administered health insurance coverage.[81] And even covered entities need not comply with HIPAA as to employment records held in their role as employer.[82] Other regimes are narrower in scope. The Americans with Disabilities Act (ADA) bars certain inquiries and examinations that would reveal employee disabilities or other health conditions.[83] Massachusetts employers cannot ask their employees about HIV status.[84] The Genetic Information Nondisclosure Act (GINA)[85] was originally passed to protect against discrimination based on the results of genetic testing,[86] but it has taken on a role as a protection against snooping around in employee's genetic data.[87] Statutes in roughly 75% of states also protect genetic information in

---

[80] 45 C.F.R. § 160.103 (2020) (defining "covered entity" as a health plan, a health care clearinghouse, or a health care provider).

[81] *See id.* §§ 164.103, 164.105; Sharona Hoffman, *Employing E-Health: The Impact of Electronic Health Records on the Workplace*, 19 KAN. J.L. & PUB. POL'Y 409, 419 (2010) ("Employers who are self-insured can receive medical information from providers for payment purposes without their employees' authorization. Such employers are considered 'hybrid' entities whose business activities include both covered (insurance) and non-covered (employment) functions.").

[82] *See* 45 C.F.R. § 160.103 (2020). In addition, covered entities may provide employee health information to employers in order "[t]o evaluate whether the individual has a work-related illness or injury." *Id.* § 164.512(b)(v)(A)(2); *see also id.* § 164.504(f) (as a condition of providing the information, the covered entity must require the employer to protect the information and not use it for employment-related actions).

[83] *See* 42 U.S.C. § 12112(d). The Seventh Circuit has held than an employer's administration of the MMPI as part of a management test was a medical examination and violated the ADA. Karraker v. Rent-A-Center, Inc., 411 F.3d 831, 832 (7th Cir. 2005).

[84] WIS. STAT. § 103.15(2).

[85] Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233, 122 Stat. 881 (codified as amended in scattered sections of 29 & 42 U.S.C.).

[86] 42 U.S.C. § 2000ff-1 (making it an "unlawful employment practice for an employer to request, require, or purchase genetic information with respect to an employee or a family member of the employee").

[87] Bradley A. Areheart & Jessica L. Roberts, *GINA, Big Data, and the Future of Employee Privacy*, 128 YALE L.J. 710, 782 (2019) ("In a world of big data, GINA offers

employment, but these have had an "extremely limited impact."[88] The notable standout is Illinois' Biometric Information Privacy Act, which provides a private right of action for improper collection, retention, or use of biometric data.[89] Finally, some states regulate the use of drug tests on employees while generally permitting it.[90]

Other pockets of employee data find their own sets of regulatory oversight. The Federal Credit Reporting Act (FCRA) requires employers to get written authorization to obtain employee credit reports; employers must also provide notice to employees if the credit report is used to take adverse action against them.[91] The FCRA only applies when employers receive or use consumer reports from consumer reporting agencies, but the term "consumer report" is construed broadly to include any information that goes to "character, general reputation, personal characteristics, or mode of living."[92] Because the FCRA largely focuses on procedural requirements of notice and consent, employers can generally comply with the statutory scheme if they follow the rules.[93] State and local legislation prohibits employers from using information of prior arrests of convections at certain points in the hiring process.[94]

---

a robust and unexpected safeguard against snooping by employers."); *cf.* Gaia Bernstein, *The Paradoxes of Technological Diffusion: Genetic Discrimination and Internet Privacy*, 39 CONN. L. REV. 241, 258 (2006) (noting that "genetic discrimination by employers and insurers is rare and is generally on the decline").

[88] Areheart & Roberts, *supra* note 87, at 763.

[89] Biometric Information Privacy Act, 740 ILL. COMP. STAT. §§ 14/1 et seq. (2009).

[90] MATTHEW W. FINKIN, PRIVACY IN EMPLOYMENT LAW 542-690 (2d ed. 2003) (describing state drug testing laws).

[91] *See* Fair Credit Reporting Act of 1970, 15 U.S.C. §§ 1681b(b)(1)-(3), 1681m. *See also* N.Y. Fair Credit Reporting Act, N.Y. Gen. Bus. L. § 380-b (regulating the use of credit reports).

[92] 15 U.S.C. § 1681a(d)(1).

[93] *See* Pauline T. Kim & Erika Hanson, *People Analytics and the Regulation of Information Under the Fair Credit Reporting Act*, 61 ST. LOUIS U. L.J. 17, 20 (2016) ("[A]lthough employers face significant liability risks if they disregard the statute's requirements, the FCRA in fact does little to curb invasive data collection practices or to address the risks of discriminatory algorithms.").

[94] MASS. GEN. LAWS ch. 151B, § 4(9), (9A).

Beyond these clumps of regulatory attention, however, employer practices are largely free from privacy-related oversight. Employer are allowed to monitor their employees as they wish; even continual electronic observation is permitted.[95] Surveillance can be tortious when conducted at private locations without the employee's consent, but observation from a public vantage is permitted.[96] An employer cannot intercept an employee's telephone or other electronic communications, even from the employer's phone, without specific consent.[97] Hidden surveillance can be legally problematic if undisclosed, but secrecy is generally permissible for

---

[95] *See* Ajunwa, Crawford & Schultz, *supra* note 18, at 747 ("There are no federal laws that expressly address employer surveillance or limit the intrusiveness of such surveillance."); *see also* Vega-Rodriguez v. Puerto Rico Telephone Co., 110 F.3d 174 (1st Cir. 1997) (permitting the use of cameras to continually survey the employees' work space).

[96] *Compare* Pemberton v. Bethlehem Steel Corp., 502 A.2d 1101, 1117 (Md. Spec. App. 1986) (holding that the use of a listening device within personal areas is generally actionable); Burns v. Masterbrand Cabinets, Inc., 874 N.E.2d 72 (Ill. App. 2007) (remanding for further proceedings on intrusion claim when the employer's investigator secretly videotaped an employee in his home after gaining entry on false pretenses), *with* ICU Investigations, Inc. v. Jones, 780 So. 2d 685 (Ala. 2000) (no intrusion when videotaped in front yard); York v. Gen. Elec. Co., 759 N.E.2d 865, 866 (Ohio App. 2001) (no intrusion when employer representative observed the employee arriving at work, going into his chiropractor's office, visiting a lawnmower repair shop, mowing his lawn, and riding a motorcycle).

[97] *See* 18 U.S.C § 2511 (2012) (criminalizing the actions of a person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication"). The tap is not illegal if one of the parties (namely, the employee) consents to the tap. *Id.* § 2511(2)(c). However, courts have not been disposed to find implied consent. Watkins v. L.M. Berry, 704 F.2d 577 (11th Cir. 1983) (notice as to employer policy of interception did not establish consent). There is also a "business extension" exception that allows for monitoring "in the ordinary course of business. 18 U.S.C. § 2510(5)(a)(i). However, listening in to personal calls is not generally within the ordinary course of business. *See Watkins*, 704 F.2d at 583. Wiretapping is also problematic under state common law. *See* Narducci v. Vill. of Bellwood, 444 F. Supp. 2d 924 (N.D. Ill. 2006) ("Eavesdropping via wiretapping has been conspicuously singled out on several occasions as precisely the kind of conduct that gives rise to an intrusion-on-seclusion claim.").

significant and legitimate business reasons, such as to catch a thief.[98] The National Labor Relations Act prohibits employer surveillance that would chill or otherwise interfere with its employees' protected concerted activity.[99] But otherwise there is no state or federal statutory regulation of employee monitoring.

Employers can also require employees to provide information as a condition of employment. In evaluating the propriety of employee interrogation, courts have looked primarily to the type of information being collected,[100] viewing more favorably data collection that is job-related, skill-related, and qualification-related.[101] Personality testing has long been a staple of employers and is not usually problematic when mainstream tests are used.[102] While questions on personality traits and emotional intelligence are seen as job-related, examinations that look beyond those elements and into

---

[98] *See* Marrs v. Marriott Corp., 830 F. Supp. 274 (D. Md. 1992) (permitting secret videotaping after hours to uncover thief); Sacramento Cty. Deputy Sheriffs' Assoc. v. Cty. of Sacramento, 59 Cal. Rptr. 2d 834 (Ct. App. 1997) (theft of inmates' property justified secret surveillance). *But see* Acuff v. IBP, Inc., 77 F. Supp. 2d 914, 927 (C.D. Ill. 1999) (videotaping nurse's office during medical exams not justified by concerns about theft).

[99] 29 U.S.C. § 158(a)(1); *see* Charlotte Garden, *Labor Organizing in the Age of Surveillance*, 63 ST. LOUIS U. L.J. 55, 60 (2018) (noting that "certain surveillance activities by employers have been illegal since the earliest days of the NLRA").

[100] W. PAGE KEETON ET AL., PROSSER AND KEETON ON TORTS § 117, at 121 (5th ed. 1984) ("[H]ighly personal questions or demands by a person in authority may be regarded as an intrusion on psychological solitude or integrity and hence an invasion of privacy.").

[101] As discussed below, these standards for examination and the requirement of job-relatedness had their genesis in the Supreme Court's discussions of examinations in the context of disparate impact in employment discrimination law. Griggs v. Duke Power Co., 401 U.S. 424, 436 (1971).

[102] The Minnesota Multiphasic Personality Inventory (MMPI), the Meyers-Briggs Type Indicator, the Rorschach Test, and the Thematic Apperception Test are among the most well-known and popular testing schema. The MMPI has been given to countless job applicants and serves as the foundation for many of the tests that employers use to assess applicants. Elizabeth D. De Armond, *To Cloak the Within: Protecting Employees from Personality Testing*, 61 DEPAUL L. REV. 1129, 1130 (2012).

confidential or demographic information may be on more shaky legal ground.[103] The federal Employee Polygraph Protection Act, along with a number of related state statutes, severely restrict the use of polygraph tests in collecting employee biometric data in response to substantive questions.[104] Relatively recent state legislation prohibits employers from requesting access to personal social-media accounts.[105]

After collecting data from workers, employers are generally able to use that data as they wish.[106] Data aggregation can reveal much more about employees than one might expect.[107] Such aggregation can feel disturbing,

---

[103] *See* Soroka v. Dayton Hudson Corp., 7 Cal. App. 77, 79-80 (1991) (asking for responses to such statements as "I feel sure that there is only one true religion. . . . I believe in the second coming of Christ. . . . My soul sometimes leaves my body. . . . I wish I were not bothered by thoughts about sex. . . . I am very strongly attracted by members of my own sex. . . . My sex life is satisfactory. . . . Many of my dreams are about sex matters.").

[104] *See, e.g.*, the Employee Polygraph Protection Act of 1988, 29 U.S.C. §§ 2001-09 (2012); D.C. CODE § 32-902; CAL. LAB. CODE § 432.2; IDAHO CODE §§ 44-903-44-904; N.J. STAT. ANN. § 2C:40A-1.

[105] Many states have legislation prohibiting employers from requiring employee disclosure of social-media passwords. ARK. CODE ANN. § 11-2-124; CAL. LABOR CODE § 980; COLO. REV. STAT. § 8-2-127; 820 ILL. COMP. STAT. § 55/10; LA. REV. STAT. 51:1953; MD. CODE, LAB. & EMP. § 3-712; MICH. COMP. LAWS § 37.273; NEV. REV. STAT. § 613.135; N.H. REV. STAT. § 275:74; N.J. STAT. ANN. § 34:6B-5; N.M. STAT. ANN. § 50-4-34; 40 OKLA. STAT. § 173.2; OR. REV. STAT. § 659A.330; R.I. GEN. LAWS § 28-56-3; TENN. CODE ANN. § 50-1-1003; UTAH CODE ANN. § 34-48-201; WASH. REV. CODE § 49.44.200; WIS. STAT. § 995.55. For a review of recent activity, see *Access to Social Media Usernames and Passwords*, NAT'L CONFERENCE OF STATE LEGISLATURES (July 1, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx.

[106] *Cf.* DANIEL SOLOVE, UNDERSTANDING PRIVACY 120 (2008) ("Most courts adhere to the secrecy paradigm, which fails to recognize any privacy interest in information publicly available or already disseminated to others.").

[107] In one example, Target used a wide variety of personal data—both generated by the store and purchased from external vendors—to develop consumer profiles including particular needs such as a pregnancy. Charles Duhigg, *How Your Shopping Habits Reveal Even the Most Personal Information*, N.Y. TIMES, Feb. 19, 2012, Magazine, at 1. Employers have successfully developed similar profiles.

even threatening, to employees, as it gives the employer an informational advantage. But there is little in the way of legal protection against such aggregation. Employers are not required to limit their use of the data for the purpose for which it was collected, or to ensure the accuracy of the data.[108] There are restrictions on disclosure. Under the "public disclosure of private facts" tort, an employer may be liable if it gives publicity to private information.[109] The duty of confidentiality generally arises from implicit or

---

Valentina Zarya, *Employers Are Quietly Using Big Data to Track Employee Pregnancies*, FORBES (Feb. 17, 2016), http://fortune.com/2016/02/17/castlight-pregnancy-data/.

[108] Bodie, Cherry, McCormick & Tang, *supra* note 32. The U.S. government is restricted as to secondary uses of data. *See, e.g.*:, Privacy Act of 1974, 5 U.S.C. § 552a(e)(3)(B) (2012). Drug testing is one exception, as the accuracy of the test has been used as one factor in considering its permissibility. *See, e.g.*:, COLO. REV. STAT. § 8-73-108(5)(e)(IX.5) (requiring the drug test to be "conducted by a medical facility or laboratory licensed or certified to conduct such tests"); IOWA CODE § 730.5.. *Cf.* Hennessey v. Coastal Eagle Point Oil Co., 609 A.2d 11, 13 (N.J. 1992) (noting that the drug test "included several features in the testing program to ensure minimum intrusion and maximum accuracy"); Sims v. NCI Holding Corp., 759 N.W.2d 333, 338 (Iowa 2009) (noting that "the legislature's intent was to ensure the accuracy of any drug test serving as the basis for adverse employment action.").

[109] RESTATEMENT (SECOND) OF TORTS § 652D (AM. LAW INST. 1977); *see also* RESTATEMENT OF EMPLOYMENT LAW § 7.05(b) (AM. LAW INST. 2015) ("An employer intrudes upon the [employee's] privacy interest . . . by providing or allowing third parties access to . . . employee information [provided in confidence] without the employee's consent."). The tort requires that the information be made public. RESTATEMENT (SECOND) OF TORTS § 652D cmt. a ("'Publicity,' on the other hand, means that the matter is made public, by communicating it to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge."). However, a line of cases has found public disclosure when there is a "special relationship" between the victim and the receivers of the private information. *See, e.g.*:, Miller v. Motorola, Inc., 560 N.E.2d 900, 903 (Ill. App. 1990) ("Where a special relationship exists between the plaintiff and the 'public' to whom the information has been disclosed, the disclosure may be just as devastating to the person even though the disclosure was made to a limited number of people."). Employees have been held to have a special relationship with their fellow employees, even when their numbers are relatively small. *Id.* ("Plaintiff's allegation that her medical condition was disclosed to her fellow employees

explicit promises, fiduciary relationships, specific statutory or regulatory requirements, or ethical rules or codes, and these may apply in certain employment relationships.[110] But employers are generally not considered to be fiduciaries of their employees' data unless they have specifically assumed that duty.[111] Once again, employers are fairly free to use worker data once collected.

Employees' privacy interests may also be infringed when employers allow their data to be accessed through faulty or negligent security systems, and certain statutes do impose security requirements on certain types of information.[112] In the 2014 Sony Pictures hack, 100 terabytes of employee data—including emails and financial, medical, and other personal information—were stolen from Sony's system.[113] Employee plaintiffs alleged that Sony's inadequate security measures allowed the hack to take place, and the case was ultimately settled.[114] Other employee claims related to

---

sufficiently satisfies the requirement that publicity be given to the private fact."); Karch v. BayBank FSB, 794 A.2d 763, 774 (N.H. 2002) (concluding that disclosure of employee's private information to employer's officers and other employees could constitute sufficient publicity).

[110] RESTATEMENT OF EMPLOYMENT LAW § 7.05, Reporters' Notes to cmt. a at 345 (AM. LAW INST. 2015).

[111] *See* Scott L. Fast, Comment, *Breach of Employee Confidentiality: Moving Toward a Common Law Tort Remedy*, 142 U. PA. L. REV. 431 (1993) (discussing the potential for the confidentiality tort in the workplace); *cf.* Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123 (2007) (comparing the broad confidentiality common-law protection in the U.K. with the overall reluctance of U.S. courts to adopt breach of confidentiality outside of limited settings).

[112] HIPAA regulations require that covered entities "protect against any reasonably anticipated threats or hazards to the security or integrity" of protected health information. 45 C.F.R. § 164.306(a)(2) (2015).

[113] Corona v. Sony Pictures Entm't, Inc., No. 14-CV-09600 RGK EX, 2015 WL 3916744, at *1 (C.D. Cal. June 15, 2015).

[114] Assoc. Press, *Sony Pictures Settles with Former Workers in Data Breach Lawsuit*, WALL ST. J. (Sept. 2, 2015, 8:49 PM ET), http://www.wsj.com/articles/sony-pictures-settles-with-former-workers-in-data-breach-lawsuit-1441241363.

unintentional disclosures have not been successful.[115] All fifty states have data breach notification laws which would apply to employers when there is a data breach involving employee personal data.[116]

B. Property Rights in Employee Data

Labor has been cited as a traditional justification for property rights—as the reason why a person should be able to own her own creation.[117] But when operating within the aegis of a firm, workers contribute their labor to the firm in exchange for payment, contributing their labor to the collective

[115] *See* Bodah v. Lakeville Motor Express, Inc., 663 N.W.2d 550 (Minn. 2003) (finding no liability when social security numbers were faxed out to sixteen different business locations); Allison v. Aetna, Inc., No. 09–2560, 2010 WL 3719243 (E.D. Pa. March 9, 2010) (dismissing complaint for lack of standing due to the absence of any injury in fact to employees after data breach.).

[116] *Security Breach Notification Laws*, NAT'L CONF. STATE LEGIS., July 17, 2020, https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx ("All 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals of security breaches of information involving personally identifiable information.").

[117] JOHN LOCKE, TWO TREATISES OF GOVERNMENT 328-29 (P. Laslett rev. ed. 1963) (3d ed. 1698) ("Whatsoever then he removes out of the State that Nature hath provided, and left it in, he hath mixed his *Labour* with, and joyned to it something that is his own, and thereby makes it his *Property*."). The post-revolutionary New Hampshire legislature justified its intellectual property law with the sentiment "there being no property more peculiarly a man's own than that which is produced by the labour of his mind." John O. McGinnis, *The Once and Future Property-Based Vision of the First Amendment*, 63 U. CHI. L. REV. 49, 80 (1996) (quoting Act for the Encouragement of Literature (1783)).

enterprise.[118] Academics have cited to this process of joint or team production as the justification for the firm itself.[119]

Intellectual property has largely followed this division of ownership in the context of employment: rights generally end up in the hands of the employer. Information produced by employees falls under the major categories of intellectual property: copyright, patent, trade secrets, trademark, and publicity. Copyright, a product of federal law, protects "original works of authorship fixed in any tangible medium of expression," such as novels, songs, and films.[120] It applies to such works when created by individuals or groups.[121] Employees generally lose copyright protection for their works when created within the context of employment. The "work-for-hire" doctrine, originally established in the 1909 Copyright Act, specified that the author of a copyrighted work "shall include an employer in the case of works made for hire."[122] The Copyright Act of 1976 modified the doctrine to make the employer the author of any work made for hire unless expressly agreed otherwise.[123] The 1976 Act defines "work made for hire" as "a work prepared by an employee within the scope of his or her employment."[124] This rule of ownership can only be altered by a signed, written document that expressly

---

[118] Lily Kahng, *Who Owns Human Capital?*, 94 WASH. U.L. REV. 607, 615 (2017) ("Although labor is always integral to the productive use of capital, intellectual capital is particularly labor-intensive and often requires workers' knowledge, experience, and skills.").

[119] Armen A. Alchian & Harold Demsetz, *Production, Information Costs, and Economic Organization*, 62 AM. ECON. REV. 777, 777-78 (1972); *see also* Margaret M. Blair & Lynn A. Stout, *A Team Production Theory of Corporate Law*, 85 VA. L. REV. 247, 249–50 (1999).

[120] 17 U.S.C. § 102.

[121] *See* Anthony J. Casey & Andres Sawicki, *Copyright in Teams*, 80 U. CHI. L. REV. 1683, 1685 (2013) (discussing the collaborative production of copyrightable material).

[122] Copyright Act of 1909, Pub. L. No. 60-349, §23, 35 Stat. 1075, 1080 (repealed 1976).

[123] 17 U.S.C. § 201(b) ("In the case of a work made for hire, the employer or other person for whom the work was prepared is considered the author for purposes of this title, and, unless the parties have expressly agreed otherwise in a written instrument signed by them, owns all of the rights comprised in the copyright.")

[124] *Id.* § 101.

changes it.[125] So when employees draft a screenplay, perform a part, or develop a software program in the context of employment, their employer owns the copyright.[126]

If copyright might be said as a general matter to concern the expression of artistic works, then patent concerns concepts relating to the useful arts. Federal law defines a patentable invention as "any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof."[127] Because patent law looks to a human inventor as the recipient of the patent rights, the employee who invents the patent is the author.[128] However, employers are free to contract with employees explicitly for the rights to all inventions created within the scope of employment. Even without an explicit contract, judges have found something akin to a work-for-hire doctrine when an employee is hired to work on a specific invention or problem; courts are more likely to conclude that "the employee was hired to invent and therefore the firm owned all patents" through an implied contract.[129] In addition, under the shop-right doctrine, employers enjoy a non-exclusive right to use the patent without

---

[125] *Id.* § 201(b).

[126] *See also* Matthew T. Bodie, *Lessons from the Dramatists Guild for the Platform Economy*, 2017 U. CHI. LEGAL F. 17, 23–24 (2017) (discussing the difference between dramatists, who work as independent contractors and own their dramatic works, and screenwriters, who work for production companies or studios and hand over their rights to those entities).

[127] 35 U.S.C. § 101.

[128] The patent must be registered by the individual inventor. See 35 U.S.C. § 111, 115 (2006) (discussing oath taken as part of patent process that the registrant is the "original and first inventor").

[129] CATHERINE L. FISK, WORKING KNOWLEDGE: EMPLOYEE INNOVATION AND THE RISE OF CORPORATE INTELLECTUAL PROPERTY, 1800-1930 180 (2009). *See also* Dan L. Burk, *Intellectual Property and the Firm*, 71 U. CHI. L. REV. 3, 15 (2004) ("In the absence of explicit contractual terms requiring an assignment, an implied duty to assign may be found. Courts have tended to recognize such an implied duty to assign patent rights in situations where an employee hired to solve a problem engages in research, and the invention relates to that effort.").

having to compensate the employee. A shop right arises when the employee has created the invention on the job using the employer's materials.[130]

To what extent is employee data included within the scope of employment even if not specifically part of the employees' contracted-for performance? Employers have been casting a wider and wider net, through by IP law and contracts, over the ideas and creations of their employees.[131] In some instances, the fights involve content that is related to the employee's primary work but arguably developed outside of the actual work relationship.[132] In other cases, the work will involve the employee but will not relate to that employee's expected work product. For example, the emails and other works within the Enron Corpus are arguably protected by copyright. If considered within the scope of work-for-hire, they would have been the property of Enron; if outside the scope, then they would belong to the individual employees. These claims have not been litigated, and the Corpus is generally considered to be abandoned material.[133] But the scope of the "scope of employment" remains up for grabs.

---

[130] FISK, *supra* note 129, at 118; Burk, *supra* note 129, at 16.

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

[132] *See id.* at 797-803 (discussing examples involving a computer algorithm and a design for a new toy line).

[133] Amana Levendowski provides the following analysis:

> The Enron emails are often colloquially referred to as being in the "public domain," but that is a legal misstatement. While the Enron emails are available online publicly, they are more like orphan works: using the works still carries some risk, as getting permission from each of the authors is highly unlikely, but the comparative likelihood of a copyright infringement lawsuit is perhaps even more unlikely. The effect is that the Enron emails are perceived as posing an infinitesimally low legal risk because, though some of the Enron emails are protectable under copyright law, the practical likelihood of former Enron employees suing for copyright infringement is exceedingly remote.

Levendowski, *supra* note 8, at 610–11.

Trade secrets have become significantly more important in the Big Data economy.[134] Protected through the common law and state statutes, trade secrets are defined as information that derives economic value from not being generally known or ascertainable and is the subject of reasonable efforts to maintain its secrecy.[135] Trade secrets can be almost any type of business information: a formula, pattern, compilation, program, device, method, technique, or process.[136] Often the result of employee labor, trade secrets may be considered to be general knowledge that can be taken by the employee when she leaves the job. The law prohibits an individual's personal or professional skills from counting as a firm's trade secrets,[137] but commentators fear that a combination of trade secret expansion and contractual provisions will sweep up employees' informational capital into the employer's domain.[138] Employees are generally presumed to have an implied duty to keep any trade secrets to which they are exposed confidential.[139] Moreover, a few jurisdictions have applied the doctrine of

---

[134] There is a lively academic debate over whether trade secrets should be consider an independent category of independent property law. *Compare* Robert G. Bone, *A New Look at Trade Secret Law: Doctrine in Search of Justification*, 86 CALIF. L. REV. 241 (1998) (arguing it does not make sense as an independent body of law); Thorton Robison, *The Confidence Game: An Approach to the Law About Trade Secrets*, 25 ARIZ. L. REV. 347, 383-84 (1983) (contending that trade secret protections should largely be contractual) *with* Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets as IP Rights*, 61 STAN. L. REV. 311, 313 (justifying trade secrets as a form of intellectual property). *See also* Michael Risch, *Why Do We Have Trade Secrets?*, 11 MARQ. INTELL. PROP. L. REV. 1, 3-4 (2007) (discussing the debate).

[135] UNIFORM TRADE SECRETS ACT § 1(4) (amended 1985), 14 U.L.A. 529 (2005).

[136] Risch, *supra* note 134.

[137] ELIZABETH A. ROWE & SHARON K. SANDEEN, CASES AND MATERIALS ON TRADE SECRET LAW 40 (2012).

[138] *See, e.g.*, Lobel, *supra* note 131.

[139] *See* Unistar Corporation v. Child, 415 So.2d 733, 734 (Fla. 3d Ct. App. 1982) ("The law will import into every contract of employment a prohibition against the use of a trade secret by the employee for his own benefit, to the detriment of his employer, if the secret was acquired by the employee in the course of his employment."); Derek P. Martin, Comment, *An Employer's Guide to Protecting Trade Secrets from Employee Misappropriation,* 1993 BYU L. REV. 949, 953 ("For most employees the law presumes a confidential relationship between employer and employee for the purposes of

"inevitable disclosure" of trade secrets to enjoin employees who (according to the court) must inevitably use the trade secrets they have learned at their old position.[140] A study of trade secret litigation found that 85% of cases involved either current or former employees or business partners.[141]

Trademarks allow a producer of goods or services to identify themselves as the source of those goods or services, and to prevent others from doing so.[142] One of the primary justifications for trademark is to allow consumers to understand where goods come from in an understandable and efficient manner.[143] At first thought, trademark might not seem to have that much to do with employee data. But trademark makes a special connection between the firm, its employees, and intellectual property. Just as patent and copyright protections allocate rights between employee and employer as to creative and useful works, trademark allocates rights as to good will and

---

protecting trade secrets."). Employers often supplement or reify this trade secret protection with contractual provisions extending employer protection to all confidential information, even beyond trade secret law. *See* Lobel, *supra* note 131, at 809.

[140] *See, e.g.*, PepsiCo v. Redmond, 54 F.3d 1262 (7th Cir. 1995); Rebecca J. Berkun, *The Dangers of the Doctrine of Inevitable Disclosure in Pennsylvania*, 6 U. PA. J. LAB. & EMP. L. 157, 157 (2003) ("The doctrine of inevitable disclosure restricts an employee's future employment if that employee will inevitably use a former employer's trade secrets in the course of the future employment.").

[141] David S. Almeling et al., *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, 45 GONZ. L. REV. 291, 294 (2010). The study also found that trade secret owners were "twice as likely to prevail on a motion for preliminary relief when they sued employees as when they sued business partners." *Id.* However, owners were also "over 70% more likely to lose a motion to dismiss when they sued employees than business partners." *Id.*

[142] 15 U.S.C. § 1127 (defining a trademark as "[a]ny word, name, symbol or device or any combination thereof [used] to identify and distinguish his or her goods, including a unique product, from those manufactured or sold by others and to indicate the source of the goods, even if that source is unknown").

[143] Mark P. McKenna, *A Consumer Decision-Making Theory of Trademark Law*, 98 VA. L. REV. 67, 73 (2012) ("According to the dominant theoretical account, trademark law operates to enable consumers to rely on trademarks as repositories of information about the source and quality of products, thereby reducing the costs of searching for goods that satisfy their preferences.").

reputation.[144] Trademarks transfer reputational assets to the firm and deprive individual employees of their ability to hold up the firm or exploit the trade dress separately.[145] Employees cannot leave their employers and still claim to be providing goods or services under the existing trademark; an employer, on the other hand, could fire every employee and still claim the same mark.

The right of publicity has been characterized both as a right to privacy[146] as well as a personal IP right—something akin to trademark for people.[147] Essentially, the right of publicity allows an individual to prevent others from using her persona—her name, image, likeness, or other indicia of identity—without consent.[148] The justifications for the right generally involve investment—financial, emotional, or moral—in one's reputation and identity.[149] Claims usually involve efforts to advertise, endorse, or provide

---

[144] Dan L. Burk & Brett H. McDonnell, *Trademarks and the Boundaries of the Firm*, 51 WILLIAM & MARY L. REV. 345, 363-64 (2009).

[145] *Id.* at 376-79.

[146] The right to publicity has its origins in tort law and was one of Dean Prosser's original four privacy torts. RESTATEMENT (SECOND) OF TORTS § 652C (AM. LAW INST. 1977) (providing protection against the appropriation of one's name or likeness). *See* Eric E. Johnson, *Disentangling the Right of Publicity*, 111 NW. U. L. REV. 891, 897 (2017) ("One such theme is that the right of publicity is said to have evolved progressively from a tort cause of action to a form of intellectual property.").

[147] Stacey L. Dogan & Mark A. Lemley, *What the Right of Publicity Can Learn from Trademark Law*, 58 STAN. L. REV. 1161 (2006); *see also* Barton Beebe, *What Trademark Law Is Learning from the Right of Publicity*, 42 COLUM. J.L. & ARTS 389 (2019) (arguing that trademark and publicity "are converging in many important ways, giving us the worst of both worlds").

[148] RESTATEMENT (SECOND) OF TORTS § 652C (AM. LAW INST. 1977) ("One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy."); Jennifer E. Rothman, *The Right of Publicity's Intellectual Property Turn*, 42 COLUM. J.L. & ARTS 277, 278 (2019) ("The right of publicity is something we all have--it is a state law that gives a person the right to stop others from using our identities--particularly our names and likenesses without permission--usually for a defendant's advantage.").

[149] Beebe, *supra* note 147, at 391 (noting the following justifications: incentivizing the creation of celebrity personas; preventing tarnishment of those personas; rewarding the labor that goes in to the development of a valuable personal identity; preventing

some other commercial use.[150] The right of publicity has not been litigated much within the employment relationship. Actors and athletes understand the value of their identity and the potential to lose control over it.[151] However, as the right of publicity has drifted closer to a property right, the ownership and assignability of identities has come into question. Employees who can assign their identities over to their employer might lose control over those identities.[152] Perhaps more than any other of these information-related rights, the right of publicity is uniquely personal.

The range of employer rights from copyright, patent, trade secrets, trademark, and publicity serve to capture a greater and greater quantity of employee data.[153] In addition to these property and/or liability rights, employers have been more and more aggressive about asserting control over employee information through contract provisions such as covenants not to compete and nondisclosure agreements.[154] Between mandatory property assignments, default rules, and employer-created contract provisions, there is very little daylight for employees to claim property rights over their employment information. Instead, firms are amassing more and more pools of worker data, putting them at risk for loss of control, displacement, and alienation.

---

misappropriation or unjust enrichment of that value; and protecting the individual liberty and dignitary interests of identity holders).

[150] RESTATEMENT (SECOND) OF TORTS § 652C cmt. b (AM. LAW INST. 1977).

[151] LATE NIGHT WITH DAVID LETTERMAN, May 30, 1983, https://www.youtube.com/watch?v=oFYeut7L2gg (interview with Carrie Fisher) (discussing Fisher's lack on input on the use of her likeness as Princess Leia in the production of toys, figurines, and shampoo bottles).

[152] Rothman, *supra* note 148, at 280. *See also* JENNIFER E. ROTHMAN, THE RIGHT OF PUBLICITY: PRIVACY REIMAGINED FOR A PUBLIC WORLD 5-6 (2018) (illustrating the dangers of assignability).

[153] Kahng, *supra* note 118, at 612 ("Intellectual capital includes not only separable, identifiable, and legally protected assets such as patents, trademarks, and copyrights, but also less distinct assets such as information systems, administrative structures and processes, market and technical knowledge, brands, trade secrets, organizational know-how, culture, strategic capabilities, and customer satisfaction.").

[154] Lobel, *supra* note 131.

III. Failing Paradigms in the Regulation of Employee Data

Even though U.S. law has taken a laissez-faire approach to the collection and use of employee data, it has provided limited protections through privacy rights and intellectual property. Ultimately, however, the entire enterprise has begun to founder on the underlying assumptions that frame these regulatory regimes. This Part examines the collapse of two primary paradigms that used to support the legal infrastructure: the separation of personal information from business-related information, and the ability of the employee to separate herself from the firm. The breakdown of these paradigms will be illustrated in two different sets of workers: drivers for ride-sharing companies like Uber and Lyft, and professional athletes. The different consequences of datafication for these two groups of workers demonstrate the importance of relative economic power in the absence of countervailing legal power.

A. The Divide between Personal and Business-Related

Law and culture in the United States have reinforced the notion that the world of work is segregable from one's personal life. Sometimes analogized as separate spheres, people are expected to have one mindset while at home and another while in the workplace.[155] The dividing line between work and home has played an important role in allowing employers fairly unlimited power with the workplace.[156] But this division rests on the shaky foundation that the work self can be separated from the personal self.

The development of data-based approach to human resources has highlighted the potential benefits of data-driven inquiries, including data that would be considered personal. The "people analytics" phenomenon involves the search for new pools of quantitative data that are correlated with business

[155] *See* Naomi Schoenbaum, *The Law of Intimate Work*, 90 Wash. L. Rev. 1167, 1174 (2015) (discussing the history of the concept).

[156] *See* Elizabeth Anderson, Private Government: How Employers Rule Our Lives (and Why We Don't Talk About It) 37-39 (2017) (describing the workplace as a dictatorship that "does not recognize a personal or private sphere of autonomy free from sanction").

and employment success.[157] Much of that data can be taken from the workplace as the employee engages in productive labor. But employers are now diving much deeper into the person's intimate physical and psychological profile. One's health affects work performance; illness can infect coworkers.[158] Companies can track and collect data on employee eye movements, heart rate, gait, speech patterns, and temperature.[159] They can see websites visited, notes sent to coworkers, likes on social media. Their understanding of employees can be much more comprehensive. And it is tempting—indeed, it may seem like good HR policy—to use that data to help workers do a better job.[160] This impulse dates back at least to Ford's Sociological Department, but the ability to act upon it has been magnified many times over.

In many fields, the line between one's personal and professional identities has been vigorously smudged. Social media is a primary culprit, as various platforms encourage a blend of work and personal connections. The examples are legion of political, cultural, or personal opinions that caused controversy on social media and led to discipline or discharge.[161] While critics bemoan the rise of "cancel culture,"[162] social media has expanded public exposure to what were heretofore private thoughts.[163] When the unpopular or offensive views become associated with the company by virtue of the

---

[157] *See* Bodie, Cherry, McCormick & Tang, *supra* note 32, at 965.

[158] Jenna Wortham, *The Down Load*, N.Y. TIMES MAGAZINE 52, 54 (Feb. 21, 2021) (noting that sick workers cost companies $575 billion in 2019, and likely significantly more in 2020).

[159] *See* Part I *supra.*

[160] *See* Wortham, *supra* note 158, at 54-56 (discussing the attraction of workplace wellness programs for employers).

[161] Bodie, *supra* note 51.

[162] Yascha Mounk, *Stop Firing the Innocent*, ATLANTIC, June 27, 2020, https://www.theatlantic.com/ideas/archive/2020/06/stop-firing-innocent/613615/.

[163] *See* Ligaya Mishan, *The Long and Tortured History of Cancel Culture*, N.Y. TIMES STYLE MAG., Dec. 3, 2020, https://www.nytimes.com/2020/12/03/t-magazine/cancel-culture-history.html (discussing the history of public sanction for unpopular opinions).

employment connection, termination often follows.[164] As a result, workers must consider the employment ramifications for almost any activity—including texts that could be screenshotted or actions that could be recorded on video and uploaded.[165] And in a twist, employees in front-facing and leadership positions are often encouraged to develop attractive social media presences and share details of their private life. Higher numbers of followers and viral posts can translate into career advantages across many occupations.

The coronavirus pandemic has exacerbated the collapse of the personal/business divide in almost every respect.[166] With shut-downs and quarantines at the outset of the pandemic, over fifty percent of workers found themselves working at home; those numbers have drifted down to about a third but are still much higher than before.[167] Using telework software allows employees to engage in their jobs but still leaves them in their homes. For those workers who must physically be present on the job, their health and the health of their coworkers has greater salience than ever. Many employers have instituted testing, tracing, and disclosure programs that monitor employee temperature, symptoms, and movements to contain the virus.[168]

---

[164] The examples are too numerous to recount. For recent examples, see Aaron Couch, Tatiana Siegel & Borys Kit, *Behind Disney's Firing of 'Mandalorian' Star Gina Carano*, HOLLYWOOD REPORTER, Feb. 16, 2021, https://www.hollywoodreporter.com/heat-vision/behind-disneys-firing-of-mandalorian-star-gina-carano; Ashley Collman, *A New York Times Editor Lost Her Job after She Tweeted about Having 'Chills' about Biden's Inauguration*, BUS. INSIDER (Jan 25, 2021, 6:36 AM), https://www.businessinsider.com/nyt-editor-lauren-wolfe-loses-job-pro-biden-tweet-2021-1; Mounk, *supra* note 162 (discussing examples).

[165] *See* Bodie, *supra* note 51 (discussing medical resident who was recorded on video mistreating an Uber driver).

[166] Wortham, *supra* note 158, at 54 ("The distinction between work and everything else, already a blurry line for most Americans, got even blurrier.").

[167] Megan Brenan, *COVID-19 and Remote Work: An Update*, GALLUP.COM, Oct. 13, 2020, https://news.gallup.com/poll/321800/covid-remote-work-update.aspx; *see also* Nicholas Bloom, *How Working from Home Works Out*, STANFORD INSTITUTE FOR ECONOMIC POLICY RESEARCH, June 2020, https://siepr.stanford.edu/research/publications/how-working-home-works-out (finding that 42% of workers were primarily working at home).

[168] *See* Bodie & McMahon, *supra* note 17.

Indeed, workers want employers to reduce the possibility of cross-infection within their ranks.[169]

This disintegration of the personal/business divide substantially weakens protections for worker data rights through privacy law and intellectual property law.[170] To a significant extent, U.S. law protects privacy within employment by drawing a line between personal information and business-related information. If that line breaks down, then so do the privacy protections.

The law already assumes that workers have little expectation of privacy while actually at work. Surveillance is presumed.[171] But technology has supercharged the ability to monitor, both in terms of quantity and quality. Employers can collect certain standard kinds of data much more easily and cheaply: phone calls are automatically logged, website URLs listed as they are visited, and video cameras can store hundreds of hours of recordings digitally.[172] The methods of collection grow ever more creative. One recent innovation is a "smart" office chair cushion that records bad posture, heart rates, and time away from the chair.[173] There seem to be limitless examples of new ways in which employers monitor and collect data from their employees.[174]

---

[169] *See NY Attorney General Letitia James Sues Amazon For Failure To Protect Workers During COVID-19 Pandemic*, EAST N.Y. NEWS, Feb. 19, 2021, https://eastnewyork.com/ny-attorney-general-letitia-james-sues-amazon-for-failure-to-protect-workers-during-covid-19-pandemic/ (lawsuit alleging that employees were disciplined or fired for raising concerns about coronavirus spread).

[170] Ajunwa, Crawford & Schultz, *supra* note 18, at 738-39 ("What is novel, and of real concern to privacy law, is that rapid technological advancements and diminishing costs now mean employee surveillance occurs both inside and outside the workplace--bleeding into the private lives of employees.").

[171] *See, e.g.*, Vega-Rodriguez v. Puerto Rico Telephone Co., 110 F.3d 174, 180 (1st Cir. 1997) ("The appellants concede that, as a general matter, employees should expect to be under supervisors' watchful eyes while at work.").

[172] Ajunwa, Crawford & Schultz, *supra* note 18, at 742-44.

[173] Tiffany May & Amy Chang Chien, *Slouch or Slack Off, This "Smart" Office Chair Cushion Will Record It*, N.Y. TIMES, Jan. 12, 2021, https: //nyti.ms/3shJ8XW.

[174] Ajunwa, Crawford & Schultz, *supra* note 18.

The law has endeavored to provide some space for personal privacy and autonomy in the workplace, but those efforts growing increasingly quixotic. Tort law has protected employees against invasions into their persons, personal space, and personal effects.[175] Workers have a reasonable expectation that employers will not surveil them in the bathroom or open up their purses or wallets without notice or consent.[176] Even offices can provide an expectation of privacy when the door is closed.[177] But the carve-out for personal privacy at work is diminishing. Workers can no longer take a moment away from a supervisor's gaze when cameras and GPS devices are always on. It may generally impermissible to record personal phone calls by workers knowingly,[178] but emails, texts, chats, listservs, and social media all preserve communications *de rigueur*. Information that was traditionally kept private because of the cost or complication in collecting it is now much more freely available.

Privacy law also has more difficulty separating work from home when the two have blended together. The observation of employees at home violates the expectation of privacy absent specific justifications, such as employer investigations of an employee's alleged disability.[179] Even in those cases, use of visual technology—binoculars, telescopic lenses—is generally forbidden.[180] But what if the employer is invited into the home through an app or a laptop? What if the employee works from home? Several states

---

[175] RESTATEMENT OF EMPLOYMENT LAW § 7.03 (AM. LAW INST. 2015) (stating that an employee has "a protected privacy interest" against employer intrusion into "the employee's physical person, bodily functions, and personal possessions").

[176] *Id.* § 7.03 cmt. b.

[177] Hernandez v. Hillsides, Inc., 211 P.3d 1063, 1073 (Cal. 2009).

[178] *See, e.g.*:, Deal v. Spears, 980 F.2d 1153 (8th Cir. 1992) (finding that recording personal employee calls violated the Wiretap Act).

[179] RESTATEMENT OF EMPLOYMENT LAW § 7.03 cmt. d (AM. L. INST. 2015) (noting that privacy interests "include nonworkplace physical or electronic locations in which the employee has a reasonable expectation of privacy, such as the employee's home, property, and personal possessions").

[180] *Id.* § 7.03 illus. 18 ("X hires an investigator to report back on employee E's off-duty activities. As part of her investigation, the investigator uses high-powered binoculars to observe E within his home. The use of high-powered binoculars to view what otherwise could not be seen is an intrusion upon E's privacy.").

require employers to follow certain protocols when electronically monitoring their employees, but these primarily require notice or consent.[181] Unlike other countries, there are no mandatory "turn off" or disconnect periods—employees can be asked to remain accessible regardless of the hour.[182] And under employment at will, employees can be terminated for their off-duty conduct, with only limited protections for political or religious activity.[183]

The personal/business divide is also critical to intellectual property law. The Enron Corpus seems like the property of the Enron Corporation and its successors in bankruptcy. The emails, calendar entries, and tasks had all been entered into the employer's Outlook system and were collected in the employer's proprietary database. It is true that individual employees might have some claims to copyright protection for "original works of authorship fixed in any tangible medium of expression."[184] But those claims would only

---

[181] California makes it a misdemeanor to use an electronic tracking device to follow the location or movement of a person without her consent. CAL. PENAL CODE § 637.7 (West 2020); *see also* Kendra Rosenberg, *Location Surveillance by GPS: Balancing an Employer's Business Interest with Employee Privacy*, 6 WASH. J. L. TECH. & ARTS 143, 149 (2010). The California Consumer Privacy Act also requires the employer to provide notice of data collection to its employees; this notice must include the type of personal information collected and its intended use also CAL. CIV. CODE §§ 1798.145(h)(3), 1798.100 (West 2020). Connecticut requires employers to provide prior written notice of the monitoring, CONN. GEN. STAT. § 31-48d (2020); *see* Gerardi v. City of Bridgeport, 985 A.2d 328, 333–35 (Conn. 2010) (statute prohibited an employer from electronically monitoring an employee's activities without prior notice). Delaware requires advance written notice which the employee must then acknowledge. DEL. CODE ANN. tit. 19, § 705(b) (2020).

[182] *Cf. French Workers Get 'Right to Disconnect' from Emails Out of Hours,* BBC.COM, DEC. 31, 2016, https://www.bbc.com/news/world-europe-38479439; Katie Way, *Workers of the World, Unplug: The Fight for the 'Right to Disconnect'*, VICE.COM (Oct. 16, 2019 2:10 p.m.), https://www.vice.com/en/article/evjk4w/right-to-disconnect-legislation-labor-movement.

[183] Matthew T. Bodie, *The Best Way Out Is Always Through: Changing the Employment at-Will Default Rule to Protect Personal Autonomy*, 2017 U. ILL. L. REV. 223, 241-58 (2017) (setting forth extant legal protections). *Cf.* RESTATEMENT OF EMPLOYMENT LAW § 7.08 (AM. L. INST. 2015) (proposing a default contractual rule against termination for political and ideological beliefs, or lawful conduct).

[184] 17 U.S.C.A. § 102(a). *See* Levendowski, *supra* note 8, at 610.

apply to extent that these emails were not written within the scope of employment, which would otherwise subsume them into the employer's property.[185]

Copyright's "work-for-hire" doctrine assumes a clean break between one's work and one's off-duty time—a break that just isn't there. The assumption then becomes that anything an employee may create that correlates in some way to the worker's job responsibilities is the employer's property. Trade secrets also allocate ideas, concepts, and data over to the employer's side of the ledger.[186] Hungry for even more of their employees' output, many companies have drafted broad assignment clauses which bolster these existing doctrines through contract. In her book *You Don't Own Me*, Orly Lobel chronicles the litigation between Mattel and a former employee over the right to Bratz Dolls, which were allegedly conceived outside of work.[187] The employee's contract required all "inventions" to be turned over to Mattel, which "includes, but is not limited to all discoveries, improvements, processes, developments, design, know-how, computer data programs, and formulae, whether patentable or unpatentable."[188]

The dissolution of the barriers between the work self and the private self has undone the traditional bargain between employer and employee. Workers no longer have a sphere where their personal, private, creative information belongs to them. The collapse of the distinction has not further atomized the players in this game; it has instead facilitated the absorption of workers into the economic system. This diffusion of the individual into the collective is our second paradigm breakdown.

B. The Embeddedness of the Worker within the Economic Firm

---

[185] 17 U.S.C. § 201(b) (work-for-hire doctrine).

[186] Camilla A. Hrdy & Mark A. Lemley, *Abandoning Trade Secrets*, 73 STAN. L. REV. 1, 8 (2021) ("It is not uncommon for someone who invented an idea while employed at a firm to want to leave and implement the idea herself if the firm won't. But currently, it's hard to do that without getting sued.").

[187] ORLY LOBEL, YOU DON'T OWN ME: HOW *MATTEL V. MGA ENTERTAINMENT* EXPOSED BARBIE'S DARK SIDE (2017).

[188] *Id.* at 22-24. The employee's new company successfully showed that the designs had evolved from the employee's original works while employed. Mattel, Inc., v. MGA Entertainment, Inc., 616 F.3d 904 (9th Cir. 2010).

Much academic attention has focused on the fissuring of the economic firm.[189] Advancements in technology, monitoring, and contracting have enabled firms to shed employees and instead to purchase labor through intermediaries.[190] A result—and likely motivation—of such fissuring is the displacement of the responsibilities of employment onto other entities. Mechanisms of fissuring include classifying workers as independent contractors, subcontracting out specific aspects of the business to smaller firms, and franchising the brand to franchisees.[191] These trends seem to signal the devolution of the firm and the weakening of its role in the economy.[192] But fissuring instead provides an example of how firms can control and utilize workers while seemingly cutting them loose. Labor is embedded within an economic system that deprives workers of their usual legal protections as well as their ability to exercise their individual autonomy. And data constructs the web that keeps these workers in place.

To continue with fissuring—it can only happen when employers can still exercise the requisite control over the work being done. The economic firm is designed to create efficiencies by bringing production under one roof, so to speak, rather than leaving it to the vagaries of the market. Ronald Coase believed that "[w]e can best approach the question of what constitutes a firm in practice by considering the legal relationship normally called that of 'master and servant' or 'employer and employee.'"[193] In Coase's view, the common law "control" test—with its notion of the employer directing the employee—was the essence of both the legal concept of "employer and employee" as well as the economic concept of the firm.[194] However, neither

---

[189] *See, e.g.*, DAVID I. WEIL, THE FISSURED WORKPLACE (2014).

[190] Brishen Rogers, *The Law and Political Economy of Workplace Technological Change*, 55 HARV. C.R.-C.L. L. REV. 531, 569 (2020).

[191] *Id.* at 569-70.

[192] *See, e.g.*, GERALD F. DAVIS, THE VANISHING AMERICAN CORPORATION: NAVIGATING THE HAZARDS OF A NEW ECONOMY (2016); June Carbone & Nancy Levit, *The Death of the Firm*, 101 MINN. L. REV. 963 (2017).

[193] R.H. Coase, *The Nature of the Firm*, 4 ECONOMICA 386, 403 (1937).

[194] *Id.* at 404.

the legal scope of the firm nor the employer-employee relationship are critical if that direction and control can be exercised without them.

Our environment of data-rich communications and analytics enables fissuring to proceed apace.[195] Firms need not hire employees if independent contractors can be nudged, adjusted, and directed by algorithms tracking their every move.[196] Hotels can hire outside housekeeping contractors and yet still ensure that workers are providing high levels of service.[197] If the law only focuses on traditional metrics of employment, such as who pays the worker, who directly supervises, who hires and fires, and whether the worker has "entrepreneurial opportunities," the end-user firm will be relieved of responsibility.[198] But these businesses still have the type of control that is necessary to develop and maintain the particular brand experience that is so essential within the modern reputation economy.[199]

Workers find themselves on the wrong end of this data revolution. They are the producers of data, but the data flows seamlessly from their work and personal experience to corporate repositories. Employers can capture the data, aggregate it into meaningful pools, analyze it, and use it to further productivity. Individual employees cannot tap into that value, nor can independent contractors. They are trapped: the more data they provide, the more powerful their employers become.

We are waking up to the transfer of power and wealth through the aggregation of data in the consumer context. Commentators have exposed

---

[195] Rogers, *supra* note 190, at 570 ("If new technologies enable a firm to ensure high-quality production through suppliers and outside contractors, that firm will have incentives to fissure away the work to reduce labor costs.").

[196] MARY L. GRAY & SIDDHARTH SURI, GHOST WORK: HOW TO STOP SILICON VALLEY FROM BUILDING A NEW GENERAL UNDERCLASS (2019) (discussing control exercised over platform-based workers).

[197] WEIL, *supra* note 189, at 145-46.

[198] FedEx Home Delivery v. N.L.R.B., 563 F.3d 492 (D.C. Cir. 2009) (expounding on the economic opportunities test for employment).

[199] In fact, the brand itself may be the primary or even singular source of value. Sonia K. Katyal & Leah Chan Grinvald, *Platform Law and the Brand Enterprise*, 32 BERKELEY TECH. L.J. 1135, 1139 (2017) (discussing "the rise of platform economies whose sole source of capital inheres in the value of the brand itself—the Airbnbs, Ubers, and eBays of the world").

the cycle of surveillance capitalism that profiles individual customers and then uses those profiles to target us for sales.[200] We understand that while these innovations have had benefits for consumers, tech companies have received extraordinary gains. And our privacy has been grievously compromised. Policymakers have begun to explore much more nuanced responses that the traditional "notice and consent" approach.[201] The California Consumer Privacy Act not only provides users explicit opt-out from data sales, but also requires data controllers to provide users with their data without charge in a format usable by other controllers.[202] Portability allows users to change companies without losing the benefits of their accumulated data over time, whether that be posts, pictures, reputation scores, or performance metrics.[203] Effectuating portability is easier in theory than in practice.[204] But at least in the consumer context, efforts to empower consumers now address the embeddedness problem, rather than simply relying on notice and consent. But we have not reached a similar point with respect to employment data.

Intellectual property law similarly ensnares workers within the mesh of the economic firm. The assignment of ownership facilitates the aggregation of data and the use of that data. When it comes to works of

---

[200] ZUBOFF, *supra* note 14.

[201] Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880 (2013).

[202] CAL. CIV. CODE § 1798.100 ("A business that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section. The information may be delivered by mail or electronically, and if provided electronically, the information shall be in a portable and, to the extent technically feasible, readily useable format that allows the consumer to transmit this information to another entity without hindrance.").

[203] Peter Swire & Yianni Lagos, *Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique*, 72 MD. L. REV. 335, 338 (2013) ("[D]ata portability can address a 'lock-in' or high switching costs problem--users start to use one service, such as Facebook, and then find it costly or technically difficult to shift to another service, even if they prefer the other service.").

[204] Engin Bozdag, Data Portability Under GDPR: Technical Challenges, Working Paper, January 28, 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3111866.

artistic expression, employers can rely on the work-for-hire doctrine to assimilate the many disparate contributions that go into a film, a website, or a media outlet. Even without the benefit of the "work-for-hire" doctrine, firms can still capture value from independent contractors through careful contracting.[205] These assignments facilitate joint creation and distribution, but they swallow up individual contributions into an undifferentiated whole.[206] In terms of data, employers can lock away their troves of employee-generated information as trade secrets. The two main criteria for identifying trade secrets—that they are valuable and they are kept secret—provide additional incentives for firms to hide their data pools.[207] State and federal laws have reinforced the legal fortress around trade secrets while still not requiring that they be registered, identified, or even defined.[208] Workers are prohibited from taking such information with them and can even be enjoined from working elsewhere for fear of inevitable disclosure.[209]

Employers are also claiming rights over employee experience, know-how, and judgment—crossing the line between the employment relationship and the individual within. Workers may spend many years building up the brand for which they labor, but they cannot claim any value over the trademark; that belongs exclusively to the employer. The worker's occupational persona is subsumed within the brand.[210] Nondisclosure agreements can prevent the worker from sharing her personal experiences on the job, closing off an avenue of individual expression whether publicly or

---

[205] Orly Lobel, *Gentlemen Prefer Bonds: How Employers Fix the Talent Market*, 59 SANTA CLARA L. REV. 663, 681 (2020).

[206] This is an overstatement; for example, screenwriters received credit for their work through a complex system of credit allocation. CATHERINE L. FISK, WRITING FOR HIRE: UNIONS, HOLLYWOOD, AND MADISON AVENUE 144-68 (2016).

[207] UNIFORM TRADE SECRETS ACT § 1(4) (amended 1985), 14 U.L.A. 529 (2005).

[208] Hrdy & Lemly, *supra* note 186.

[209] Ryan M. Wiesner, *A State-by-State Analysis of Inevitable Disclosure: A Need for Uniformity and a Workable Standard*, 16 MARQ. INTELL. PROP. L. REV. 211 (2012).

[210] *See also* Marion Crain, *Managing Identity: Buying into the Brand at Work*, 95 IOWA L. REV. 1179, 1184 (2010) ("Internal branding programs utilize a coordinated hiring, training, disciplinary, and reward structure to imprint brand values upon workers' identities and create an emotional connection with the firm so that the boundaries between employees' own interests and those of the firm begin to blur.").

privately.[211] Covenants not to complete and their associated cadre of noncompetition clauses foreclose the exploration of opportunities outside the firm and further limit worker efforts to exercise autonomy in the economic sphere.[212]

The concentration of intellectual property rights within a firm makes some economic sense. Joint production can be impossible without a central rights-holder to manage the process. Armen Alchian and Harold Demsetz conjectured that the purpose of the firm was not to control, but rather to manage a diverse set of contributions that are difficult to compare or segregate.[213] Under their theory, team production is "production in which 1) several types of resources are used and 2) the product is not a sum of separable outputs of each cooperating resource."[214] An independent monitor—the firm—would insure that the team members all contribute appropriately and are rewarded appropriately.[215] The difficulty here is that firms are not accountable to those who provide the labor. The result is that firms capture the value provided by employees while remaining unaccountable to them for that value.[216]

Worker data is valuable. But existing legal regimes facilitate the disconnection of employees from their data in its collection, aggregation, and use. Most employers have enjoyed almost unlimited authority in their control and profit from the new data economy. In some circumstances, however,

---

[211] Lobel, *supra* note 205, at 681 (discussing how NDAs can expand "beyond the traditional categories of trade secrets, include general know-how, client lists, and salary information").

[212] Lobel, *supra* note 131, at 824-34.

[213] Alchian & Demsetz, *supra* note 119, at 777-78.

[214] *Id.* at 779.

[215] *Id.* at 782–83.

[216] *See* Dan L. Burk & Brett H. McDonnell, *The Goldilocks Hypothesis: Balancing Intellectual Property Rights at the Boundary of the Firm*, 2007 U. ILL. L. REV. 575, 635 (2007) ("We have seen why the law might best assign [intellectual property] rights to firms in such circumstances. However, this leaves employees open to exploitation, so that the opposite assignment might be better. Even if assigning rights to the firm is best, it is possible that protection of employees then requires assigning more power to employees within firms than we observe.").

workers have overcome the default distribution to play a larger role in data processing and collect more of its rewards. We turn next to examples of both.

C. The Digital Divide: Platform Drivers and Professional Athletes

Worker efforts to disentangle themselves from their economic and legal systems and regain some control over their data may appear hopeless. There is a sense of doom, of resignation, in reflections on the declining expectations of privacy and the powerlessness of employees to resist it.[217] This despair is warranted considering the technological advances that facilitate privacy compromise and value displacement. But some workers have managed to harness, if not fully capture, the ways in which data can be used to enhance workplace productivity.

Most workers are not in that position. Employers have largely been left to their own devices to collect and use employment data as they see fit. The platform ride-sharing companies such as Uber and Lyft represent an extreme version of this relationship. These companies have come as close as possible to distilling their core businesses down to big data operations.[218] They pitch themselves as technology companies or platform providers, not transportation service providers.[219] The data relationship forms a cycle: the companies collect information from the drivers and passengers, and then the companies use that information to set prices and incentivize drivers to meet

---

[217] Ajunwa, Crawford & Schultz, *supra* note 18, at 776 (noting that workplace surveillance innovations "have decimated worker privacy"); J.S. Nelson, *Management Culture and Surveillance*, 43 SEATTLE U. L. REV. 631, 635 (2020) (discussing "how much more invasive technological surveillance has become").

[218] ALEX ROSENBLAT, UBERLAND: HOW ALGORITHMS ARE REWRITING THE WORLD OF WORK 3 (2018) ("At its core, Uber does one thing really well: it organizes work for drivers and rides for passengers through its smartphone app.").

[219] Joel Rosenblatt, *Uber's Future May Depend On Convincing the World Drivers Aren't Part of its 'Core Business,'* TIME (Sept. 12, 2019 9:37 AM EDT), https://time.com/5675637/uber-business-future/ ("'Drivers' work is outside the usual course of Uber's business, which is serving as a technology platform for several different types of digital marketplaces,' Tony West, the company's chief legal officer, said in an interview with reporters Wednesday.').

passenger needs. The process is all managed by sophisticated algorithms that feed on massive amounts of data.[220]

Platform companies garner a vast trove of data from their workforce. They track location data to deploy drivers who are closest to customers.[221] But along with tracking locations, the companies provide directions to drivers, and they track how effective those directions are over time.[222] In fact, Uber has been known to designate a certain ride for exploration in which the driver takes a less-traveled route to "map" that possibility for the machine.[223] This is just one example of the ways in which platform companies may manipulate drivers and customers by implying something about the data that just isn't there.[224] The companies also track other types of data about drivers, including reputation scores from customers,[225] how long drivers are idle without engaging in a compensated ride,[226] and even the physical stability of the phone within the car.[227] Drivers must put their trust in the companies to manage this data, despite failures in security.[228]

Although drivers build this system with their data, they find themselves disempowered through their data relationship. Information is collected by the platform companies and largely disappears from individual

---

[220] ROSENBLAT, *supra* note 218, at 3 ("Rather than supervising its hundreds of thousands of drivers with human supervisors, the company has built a ride-sharing platform on a system of algorithms that serves as a virtual 'automated manager.'").

[221] *Id.*

[222] *Id.* at 132.

[223] *Id.* at 133.

[224] *Id.* at 114-25 (discussing examples); *see also* Sarah Mason, *High Score, Low Pay: Why the Gig Economy Loves Gamification*, GUARDIAN, Nov. 20, 2018, https://www.theguardian.com/business/2018/nov/20/high-score-low-pay-gamification-lyft-uber-drivers-ride-hailing-gig-economy (discussing how Lyft motivates drivers through gamification).

[225] *Id.* at 149-56.

[226] Sarah Holder, *For Ride-Hailing Drivers, Data Is Power*, BLOOMBERG CITYLAB, Aug. 22, 2019, https://www.bloomberg.com/news/articles/2019-08-22/why-uber-drivers-are-fighting-for-their-data.

[227] ROSENBLAT, *supra* note 218, at 141-42.

[228] *Id.* at 163-64.

drivers' purview.[229] Meanwhile, the platform companies use algorithms to manage drivers and provide only automated and inexpensive technical or managerial assistance.[230] So the process is dehumanizing in two respects: workers not only interact primarily with an algorithm that controls their daily experience, but their own data is the raw material that builds and sustains that algorithm. It is a black box that the workers create but have no control over or institutional connection to.

Lack of driver power within the data relationship has motivated efforts to change the equation. Drivers in the United Kingdom have asserted their rights to obtain and manage their data under the General Data Protection Regulation (GDPR), a European Union privacy regulation that went into effect in 2018.[231] In particular, they want data portability—a right under the GDPR—to obtain their data for their own purposes.[232] In the United States, the Driver's Seat Cooperative provides an app allowing drivers to turn on a GPS system that runs in the background while they work, recording their location.[233] The Cooperative plans to aggregate, anonymize, and share the data with participating drivers.[234] If drivers do not obtain some level of control over either their data or the platform companies themselves, they may find themselves out of work altogether, as the companies are using this data to build systems with self-driving cars.[235] The drivers are supplying the raw materials for this new automated system through their data—their labor—without any stake in its future success.

---

[229] Holder, *supra* note 226 (quoting a drivers as to his efforts to get his data to "assert my rights and eliminate the asymmetry in information power between me and Uber").

[230] DANIEL LYONS, LAB RATS: HOW SILICON VALLEY MADE WORK MISERABLE FOR THE REST OF US 150 (2018); ROSENBLAT, *supra* note 218, at 144.

[231] Holder, *supra* note 226; *Uber Drivers Demand Their Data*, ECONOMIST, MAR. 20, 2019, https://www.economist.com/britain/2019/03/20/uber-drivers-demand-their-data.

[232] *Id.*

[233] Holder, *supra* note 226.

[234] *Id.*

[235] Kirsten Korosec, *Lyft Is Using Data from its Rideshare Drivers to Develop Self-Driving Cars*, TECHCRUNCH.COM (June 23, 2020, 10:51 AM CDT), https://techcrunch.com/2020/06/23/lyft-is-using-data-from-its-ride-share-drivers-to-develop-self-driving-cars/.

More data is likely collected from professional athletes than any other occupation. "People analytics" began in baseball in 1859 with the first box score.[236] Ever since, professional athletes have been observed in every aspect of their performance on the field.[237] The *Moneyball* phenomenon brought new sets of data and data analytics to the evaluation of players, and the search for untapped information continues apace.[238] Player movements are chronicled with video recordings that capture 25 frames per second.[239] New statistics are constantly developed to capture all aspects of performance.[240] But the search for performance metrics has long since moved beyond what happens on the court or field. Monitoring now goes on 24 hours a day.[241] The types of data are staggering: body and eye movements, elbow stress, skin temperature, heart rate, oxygen levels, glucose levels, hydration, sleep

---

[236] Mike Pesca, *The Man Who Made Baseball's Box Score a Hit*, NPR.ORG, July 30, 2009, https://www.npr.org/templates/story/story.php?storyId=106891539.

[237] Former professional quarterback Peyton Manning lampooned the extreme fan attention given to players' performance in his "Cut that meat!" ad. Steve Gardner, *Peyton Manning's Top 10 TV Commercials in Honor of His 44th Birthday*, USA TODAY (Mar. 24, 2020 7:30 A.M. ET), https://www.usatoday.com/story/sports/nfl/2020/03/24/peyton-manning-10-best-tv-commercials-nfl-nationwide-espn/2903386001/.

[238] LEWIS, *supra* note 33; Terrance F. Ross, *Welcome to Smarter Basketball*, ATLANTIC, June 25, 2015, https://www.theatlantic.com/entertainment/archive/2015/06/nba-data-analytics/396776/ ("Every micro-movement on the court could now be tracked, quantified, and eventually archived. No longer could a player 'hide' his deficiencies on the court.").

[239] Ken Berger, *Warriors 'Wearable' Weapon? Devices to Monitor Players While on the Court,* CBS SPORTS, (June 3, 2015, 7:41 A.M. ET), https://www.cbssports.com/nba/news/warriors-wearable-weapon-devices-to-monitor-players-while-on-the-court/.

[240] *The NBA's Adam Silver: How Analytics Is Transforming Basketball*, KNOWLEDGE@WHARTON, June 1, 2017, https://knowledge.wharton.upenn.edu/article/nbas-adam-silver-analytics-transforming-basketball/ (discussing efforts to record assists of assists).

[241] *Id.* ("At night, most players wear sleep monitors.").

rhythms.[242] The avalanche of data techniques and analytics has led to the "hyperquantified athlete."[243]

These immersive levels of surveillance create the impression that these workers are trapped in a dystopian, Orwellian environment. And to be sure, players have chafed at the invasiveness of many protocols.[244] But in looking at the bigger picture, professional athletes have facilitated the use of their data in ways that inure to their benefit. To begin with, they are extremely well-compensated. The minimum salaries in the four major men's sports leagues are all in the range of a half-million dollars and accelerate quickly thereafter.[245] The interest in data reflects the money generated by professional sports, and players have managed to secure a significant chunk of that revenue. Because all four major leagues are unionized, players also have a collective voice to negotiate the methods, manner, and scope of data collection by the teams.[246] There is some concern that the players' unions have not kept up with the latest developments in data collection, particularly

---

[242] Nick Busca, *As Biometrics Boom, Who Owns Athletes' Data? It Depends on the Sport.,* WASH. POST (Feb. 2, 2021 7:00 A.M. CST), https://www.washingtonpost.com/sports/2021/02/02/athletes-biometrics-data-privacy/; Travis Sawchik, *Pirates Look to Create, Measure Optimum Performance*, PITTSBURGH TRIB., July 16, 2016, https://archive.triblive.com/sports/pirates/pirates-look-to-create-measure-optimum-performance/ (discussing the Omega Wave technology); *Oura Partners With WNBA for 2020 Season*, BUSINESSWIRE.COM (July 30, 2020 9:00 a.m.), https://www.businesswire.com/news/home/20200730005532/en/%C2%A0Oura-Partners-With-WNBA-for-2020-Season.

[243] David Jarvis, Kevin Wescott & Dan Jones, *The Hyperquantified Athlete: Technology, Measurement, and the Business of Sports, in* DELOITTE INSIGHTS: TECHNOLOGY, MEDIA, AND TELECOMMUNICATIONS PREDICTIONS 2021 (2020), file:///C:/Users/sambl/Downloads/DI_2021-TMT-predictions.pdf.

[244] Rian Wyatt, *New Technologies Are Forcing Baseball To Balance Big Data With "Big Brother*," VICE (May 27, 2016 9:20 A.M.), https://www.vice.com/en/article/8qygbp/new-technologies-are-forcing-baseball-to-balance-big-data-with-big-brother.

[245] Connor Fleming, *How Do The Minimum MLS And NWSL Salaries Compare To Other U.S. Sports?*, THE18.COM, Feb. 6, 2019, https://the18.com/en/soccer-entertainment/minimum-salary-in-pro-sports.

[246] 29 U.S.C. § 158(a)(5) (setting forth the duty to bargain).

with respect to health data.[247] But worker data falls under the terms and conditions of employment, which means the leagues must bargain with the unions about them.[248] Collective bargaining agreements in professional sports provide players with control and ownership over certain kinds of data.[249] In addition, individual players have significant ownership rights over the uses of their names and likenesses. Although the leagues have the power to make collective agreements over their use, players retain significant individual rights to participate in advertisements, endorsements, and other opportunities to trade on their individual and team success.[250]

Even with their individual and collective market power, athletes are still pressing for stronger rights over their data. Many teams make data analytics innovations voluntary on the part of the player, but collective bargaining agreements could be stricter on their use and could forbid the more invasive technologies.[251] Players have also banded together to seek control and ownership of their data outside the collective-bargaining context. In the United Kingdom, Project Red Card seeks to reclaim rights over player statistics from the many outside analysts and gambling agencies that process that data for their own economic benefit.[252] These athletes claim that the GDPR renders the processing illegal without their consent.[253]

---

[247] Skyler R. Berman, *Bargaining Over Biometrics: How Player Unions Should Protect Athletes in the Age of Wearable Technology*, 85 BROOK. L. REV. 543, 545 (2020).

[248] *See* NLRB v. Wooster Div. of Borg-Warner Corp., 356 U.S. 342, 349 (1958) (explain the difference between mandatory and permissive subjects of collective bargaining).

[249] Busca, *supra* note 242.

[250] Perhaps the most important publicity-rights case involved baseball cards. Haelan Labs., Inc. v. Topps Chewing Gum, Inc., 202 F.2d 866 (2d Cir. 1953).

[251] Berman, *supra* note 247, at 545-46.

[252] Nick Hartley & Philip Marsh, *Russell Slade: Ex-Manager Leads Lawsuit over use of Players' Personal Data*, BBC.COM, July 28, 2020, https://www.bbc.com/sport/football/53557706; David Ornstein, *Players to Sue for Hundreds of Millions over Use of Their Statistics*, ATHLETIC, July 26, 2020, https://theathletic.com/1949883/.

[253] Hartley & Marsh, *supra* note 252 ("Using the requirements placed by the General Data Protection Regulations brought in in 2018, players will claim that they have neither given consent, nor received the chance to change data they feel

Even with these concerns, data analytics are not necessarily viewed by athletes solely as a burden to bear. Players in less well-funded leagues see the absence of analytics as problematic and want their leagues to invest in them.[254] After all, the purpose of these analytics is generally to improve the players' performance, maximize playing ability, and prevent injury.[255] These technologies can make players safer and healthier, stronger and swifter, smarter and savvier. They should be a win-win. But players need voice and power to avoid the opportunistic and voyeuristic aspects of monitoring regimes controlled exclusively by employers.

The examples of ride-sharing drivers and professional athletes show that concerns about the collection and use of worker data do not simply fall along a metric from more invasive to less invasive. The nature and scope of the data processing matter, but so do the purposes of the processing and the worker control and ownership over it. If workers can participate in the design of the data program, object when it goes too far, and then better themselves through the program, then data analytics is a positive development. These principles should guide us as we reimagine the legal regime for all workers.

IV. A New Regime for Worker Data: Privacy, Property, and Governance

Traditional paradigms within the employment relationship are breaking down. Lines are blurring between personal and business-related, and between worker and firm. Existing regimes of legal categorization and calibration no longer hold (if they ever really did). We need to rethink our approach to employee data and our regulation of the relationship between

misrepresents them, nor have they been given the chance to be either reimbursed for their use or taken out of it entirely—all staples of the GDPR rules.").

[254] *See* Taylor Soper, *Basketball Legend Sue Bird on the Data Disparity between Men's and Women's Sports*, GeekWire.com (March 16, 2016, 4:14 A.M.), https://www.geekwire.com/2016/basketball-legend-sue-bird-data-disparity-mens-womens-sports/.

[255] Ron Miller, *NFL-AWS Partnership Hopes to Reduce Head Injuries with Machine Learning*, TechCrunch.com (Dec. 5, 2019 4:24 PM CST), https://techcrunch.com/2019/12/05/nfl-aws-partnership-hopes-to-reduce-head-injuries-with-machine-learning/.

worker and firm. This Part will explore three potential avenues for adapting to the new environment: (a) creating a hybrid approach to employee data regulation, melding aspects of both privacy law and property law; (b) recognizing employers as information fiduciaries with respect to employee data; and (c) providing for worker participation in the firm's informational governance.

A. A Hybrid Approach to the Privacy/Property Conundrum

The collection and use of employee data falls under two distinct U.S. legal regimes: privacy and property. Privacy protections generally apply to an employee's non-public, personal data, such as health and biometrics, personal communications, and political or religious beliefs. But such protections can also apply, to a very limited extent, within the workplace itself. In contrast, instances of employee data creation that can be categorized as property are assigned to the firm. Both systems cover information that is "related to" the employee but provide sharply different ways of regulating its use.

The best way forward as to all varieties of employee data is to blend the privacy and property approaches—something that individual legal doctrines themselves often do.[256] A hybrid approach to employee data protection recognizes that employees have continuing interests in the use of their data. In some situations, they will want to shield the data from further disclosure or analysis. In other situations, they will want credit for the data and a chance to participate in its continuing creation of value.[257] But these interests are not an either/or switch. Information that is traditionally considered personal may have value to the business, and creative expressions

[256] *See, e.g.*:., Daniel A. Crane, *Intellectual Liability*, 88 TEX. L. REV. 253, 255 (2009) (examining whether intellectual property regimes are truly "property" or rather a hybrid form of property and liability).

[257] One example of continuing interests in property, even after it is no longer owned by the individual, is the Visual Artists Rights Act of 1990 (VARA), 17 U.S.C. § 106A (2000). VARA provides visual artists with three "moral" rights over their art: the right of integrity to prevent any intentional distortion, mutilation, or other modification;" the right of attribution; and the right to prevent the destruction of works of visual art that are "of recognized stature." *Id.* For an argument against such rights, see Amy M. Adler, *Against Moral Rights*, 97 CAL. L. REV. 263, 300 (2009).

or personal identity may need ongoing privacy protections against intrusions. A regulatory regime that melds aspects of privacy law and intellectual property law—for employee data as a whole—is necessary in the information economy.

A system constructed purely around privacy regulation fails to account for the unique features of the employment relationship. Privacy law focuses on the collection of information and imposes legal barriers to access when physical or electronic barriers fail.[258] The traditional common-law intrusion tort largely imagines an invasion from the outside—a nonconsensual violation.[259] But there are steady and significant flows between employers and employees covering a wide variety of information. Even the disclosure of extremely private information can at times be necessary.[260] It is hard to find absolutes here.[261] And it is inappropriate to borrow too much from consumer privacy regimes; although consumers may have ongoing data relationships, the information flow is generally not as thick and constant as between employee and employer.

Property rights are meant to be more concrete and definable, as compared to privacy.[262] The property has an owner, and that owner has certain rights over the property regarding its use. This clarity is invaluable when it comes to real property, as parties and courts need to know who has the right to use, exclude, and sell.[263] In the context of the employment relationship, however, this move towards enclosure creates difficulties.

---

[258] RESTATEMENT OF EMPLOYMENT LAW § 7.03 (AM. LAW INST. 2015).

[259] RESTATEMENT SECOND OF TORTS § 652B (AM. LAW INST. 1977).

[260] For an extreme example, see Feminist Women's Health Ctr. v. Superior Court, 52 Cal. App. 4th 1234 (1997).

[261] Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 562 (2006) ("Protecting privacy requires careful balancing, as neither privacy nor its countervailing interests are absolute values.").

[262] *See, e.g.*, Bernstein, *supra* note 87, at 253 ("Privacy is considered a vague and protean concept.").

[263] *See, e.g.*, Henry E. Smith, *Intellectual Property as Property: Delineating Entitlements in Information*, 116 YALE L.J. 1742, 1793–94 (2007). But this clarity can be overstated. *See, e.g.*, LEE ANNE FENNELL, SLICES & LUMPS: DIVISION AND AGGREGATION IN LAW AND LIFE (2019) (discussing different aggregations of property rights).

Property law allows one party—almost always the employer—to claim exclusive rights over the information. In all areas of intellectual property—trademark, copyright, patent, trade secrets, and publicity—businesses are aggressively asserting their rights over employees and capturing all of the economic value from this jointly-contributed resource.

The strengths and weakness of these approaches has played out in the larger struggles over the management of personal data. Some commentators have proposed a system of property rights in data in order to give their creators more control over its use as well as an opportunity to participate in the value that their data creates.[264] However, reception to this idea has largely been negative.[265] Property rights would (further) restrict the free flow of information, inhibiting the spread of knowledge and understanding.[266] If the rights were alienable, personal data could easily come under the control of another—in our case, the employer.[267] If inalienable, they would allow for the

---

[264] *See, e.g.*, Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2056 (2004). ("This Article develops the five critical elements of a model for propertized personal information that would help fashion a market that would respect individual privacy and help maintain a democratic order. These five elements are: limitations on an individual's right to alienate personal information; default rules that force disclosure of the terms of trade; a right of exit for participants in the market; the establishment of damages to deter market abuses; and institutions to police the personal information market and punish privacy violations."); A. Michael Froomkin, *The Constitution and Encryption Regulation: Do We Need a "New Privacy" ?*, 3 N.Y.U. J. LEGIS. & PUB. POL. 25, 34 (1999) (suggesting an intellectual property model for data privacy).

[265] Amy Kapczynski, *The Law of Informational Capitalism*, 129 YALE L.J. 1460, 1501 (2020) ("Intellectual-property scholars have, for the most part, argued vociferously against any form of property protection in personal data for a variety of reasons, including concerns about transaction costs and innovation.").

[266] *See* Lothar Determann, *No One Owns Data*, 70 HASTINGS L.J. 1, 5 (2018) ("New property rights in data are not suited to promote better privacy or more innovation or technological advances, but would more likely suffocate free speech, information freedom, science, and technological progress.").

[267] *See* ROTHMAN, *supra* note 152, at 136-37 (discussing the dangers of the right to sell one's right of publicity); Pamela Samuelson, *Privacy As Intellectual Property?*, 52 STAN. L. REV. 1125, 1171 (2000) ("Also mismatched are traditional policies of

creation of an anticommons.[268] Any such regime would also raise significant logistical issues[269] and free speech concerns.[270]

Separating out individualized data property cuts against the purpose of the firm—namely, to enable joint production. Firms are used when joint production facilitates productivity.[271] The participants in this unit—the firm—have cast their lots together to engage in economic activity that would otherwise be extremely difficult to tease out into separate contracts. Because these players are all working together, they are treated as a unit for certain

---

property law favoring free alienability and information privacy policy preferences for restrictions on alienation.").

[268] *See* Mark A. Lemley, *Private Property*, 52 STAN. L. REV. 1545, 1550 (2000) ("Ownership rights presumably will have to exist in bits of data, so we might want to grant individuals ownership over even seemingly innocuous bits of data which might be aggregated later on. But the more broadly we define the right, the more we will interfere with everyday commerce."); Jane Yakowitz, *Tragedy of the Data Commons*, 25 HARV. J.L. & TECH. 1, 2 (2011) (discussing the benefits to research from a data commons). On the anticommons, see Michael A. Heller, *The Tragedy of the Anticommons: Property in the Transition from Marx to Markets*, 111 HARV. L. REV. 621, 624 (1998) ("In an anticommons, by my definition, multiple owners are each endowed with the right to exclude others from a scarce resource, and no one has an effective privilege of use. When there are too many owners holding rights of exclusion, the resource is prone to underuse—a tragedy of the anticommons.").

[269] Determann, *supra* note 266, at 5 ("[T]here is much uncertainty and ambiguity regarding the meaning of 'data,' 'information,' and 'ownership;' little comprehensive analysis regarding how existing properly laws already cover data or exclude data from protection; and relatively sparse considerations of legal and policy reasons for not granting properly rights to data.").

[270] *See* Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57, 60 (2014) ("When the government deliberately interferes with an individual's effort to learn something new, that suppression of disfavored knowledge is presumptively illegitimate and must withstand judicial scrutiny."); Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049 (2000).

[271] Alchian & Demsetz, *supra* note 119, at 780.

purposes.[272] The coordinating aspects of firm production allow for the whole to be greater than the sum of the parts.[273]

This unique informational relationship calls for a hybrid approach. The foundations of such an approach would have three characteristics. First, employees would have ongoing rights in their data even after providing it to the employer. These rights would be similar to those provided under the European Union's General Data Protection Regulation (GDPR).[274] The rights include:

---

[272] Guy Davidov has recognized that the concept of employee requires a governance structure (such as a firm) outside of the market. He argues that structure is necessary as "a direct result of two combined factors: first, our inclination to join forces and work together with others; and second, the need to coordinate production to an extent that the market cannot satisfy." Guy Davidov, *The Three Axes of Employment Relationships: A Characterization of Workers in Need of Protection*, 52 U. TORONTO L.J. 357, 377-78 (2002).

[273] Indeed, the data itself may the production of the team members as a group, even if it involves data related to individual members of the team. As Amy Kapczynski has elaborated:

> The tendency instead to see data as a thing that springs from a person and that enters the world as a transcendent object misapprehends what data is and obscures how it came to serve as a critical form of capital in the current age. This view of data—rather like the view of commodities of which Marx once wrote—imbues it with a kind of religious aura, treating "productions of the human brain" as if they are "autonomous figures endowed with a life of their own, which enter into relations both with each other and with the human race." If we are to intervene to democratize private power today, we must instead understand data (and by extension, information and knowledge) as the product of social relations and so properly the object of social interest. And we must understand how law helps to construct data, and data as capital, by shaping these social relations.

Kapczynski, *supra* note 265, at 1499 (footnotes omitted).

[274] Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC,

- A right to be notified about data collection (Article 12);
- A right to access and review one's data (Article 15);
- A right to correct erroneous data (Article 16);
- A right to have irrelevant or misleading data deleted (Article 17);
- A right to restrict use of the data to the purpose for which it was originally collected or provided, unless further consent is provided (Article 5); and
- A right of portability—the ability to obtain and take one's data from the employer (Article 20).[275]

These rights do not require "privacy" in the traditional American sense of fencing off certain information from access.[276] Rather, they are rights to control the use of one's data even after it is in another's hands.[277] These are exactly the kinds of rights that employees need when they have an interest in providing the data but also an interest in the use thereafter.

Arts. 1, 9 (General Data Protection Regulation), 2016 O.J. (L 119) (EU) [hereinafter GDPR]. An easily accessible version of the GDPR can be found at: Intersoft Consulting, GDPR, https://gdpr-info.eu/.

[275] *Id.*

[276] The GDPR protects against inappropriate data collection through Article 6, which requires a specific justification for any "processing," which would include collection. GDPR, *supra* note 274, Art. 6. Consent is one such justification. However, the GDPR has essentially said that consent cannot be trusted in the employer-employee relationship because of the power imbalance between the parties. *Id.*, Recital 42(1) (discussing the employment relationship as an example of "a clear imbalance between the data subject and the controller" under which consent is suspect). Acknowledging the need for data processing within the employment relationship, GDPR guidance indicates that much of such processing will be justified either as necessary to the relationship or as an appropriate balance between the interests of the parties. Article 29 Data Protection Working Party, *Opinion 2/2017 on Data Processing at Work*, 17/EN WP 249, at 6-8 (June 8, 2017), http://ec.europa.eu/newsroom/document.cfm?doc_id=45631.

[277] Jacob M. Victor, *The EU General Data Protection Regulation: Toward A Property Regime for Protecting Data Privacy*, 123 YALE L.J. 513, 516 (2013) ("The draft Regulation seems to transcend this debate by adapting the rights and remedies commonly associated with property in service of a human-rights-driven approach to privacy.").

Second, employees should also have ongoing rights over the value generated by the data use. In particular, additional or unexpected income from the use of the data should not be expropriated without some system of sharing. There are reports of employers bundling and selling employee data to third parties for uses unassociated with joint production.[278] These sales should be prohibited without employee consent, and employers should be prohibited from punishing workers who refuse to give their consent for resale.

Third, protections would kick in against employer's collection or use of data that transgressed societal norms of dignity and decency.[279] There is still plenty of information that employees wish to keep out of the hands of their managers and co-workers. Traditional tort law can continue to police these boundaries, but a broader federal law with more clarity as to scope would be a welcome development.[280] Regardless, we can no longer expect traditional privacy protections against information collection to do all the work for us when it comes to employee data. Instead, we should recognize that employees have ongoing privacy and (quasi-)property rights in their data, and that the law should recast itself accordingly.

B. Employers as Information Fiduciaries

Another way to regulate the collection and use of employment data would be a more rigorous set of employer duties concerning the stewardship of this data. The law already has a method for placing heightened responsibilities on actors for the care of others: fiduciaries. When exercising control or possession over things that belong to another, a fiduciary has heighted obligations to care for those things and not to betray the trust of the owner.[281] Courts and commentators have characterized the exercise of control

---

[278] Adler-Bell & Miller, *supra* note 15.

[279] *See, e.g.*, Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 138 (2004) (arguing that privacy protections serve to enforce norms of information appropriateness and norms of information flow or distribution).

[280] Ajunwa, Crawford & Schultz, *supra* note 18, at 773-75.

[281] Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1207 (2016) ("A fiduciary is one who has special obligations of loyalty and trustworthiness toward another person.").

by the fiduciary in different but related ways: the ability of the fiduciary to exercise discretion in carrying out its tasks;[282] the vulnerability of the beneficiary to the fiduciary's exercise of power and potential opportunism;[283] the trust and confidence reposed in the fiduciary by the beneficiary;[284] and reasonable expectations of the parties.[285] The employment relationship fits

[282] Zastrow v. Journal Commc'ns, Inc., 718 N.W.2d 51, 59 (Wis. 2006) ("A consistent facet of a fiduciary duty is the constraint on the fiduciary's discretion to act in his own self-interest because by accepting the obligation of a fiduciary he consciously sets another's interests before his own."); Paul B. Miller, *A Theory of Fiduciary Liability*, 56 MCGILL L.J. 235, 262 (2011) (describing a fiduciary relationship as "one in which one party (the fiduciary) enjoys discretionary power over the significant practical interests of another (the beneficiary)"); D. Gordon Smith, *The Critical Resource Theory of Fiduciary Duty*, 55 VAND. L. REV. 1399, 1402 (2002) ("[F]iduciary relationships form when one party (the 'fiduciary') acts on behalf of another party (the 'beneficiary') while exercising discretion with respect to a critical resource belonging to the beneficiary."); s*ee also* D. Gordon Smith & Jordan C. Lee, *Fiduciary Discretion*, 75 OHIO ST. L.J. 609, 644 (2014) ("The most commonly cited scholarly works in the canon of fiduciary law emphasize the importance of discretion in fiduciary relationships.")..

[283] Burdett v. Miller, 957 F.2d 1375, 1381 (7th Cir. 1992) ("The common law imposes that [fiduciary] duty when the disparity between the parties in knowledge or power relevant to the performance of an undertaking is so vast that it is a reasonable inference that had the parties in advance negotiated expressly over the issue they would have agreed that the agent owed the principal the high duty that we have described, because otherwise the principal would be placing himself at the agent's mercy.").

[284] Wiener v. Lazard Freres & Co., 672 N.Y.S.2d 8, 14 (N.Y. App. Div. 1998) (inquiring as to whether one party "reposed confidence in another and reasonably relied on the other's superior expertise and knowledge").

[285] Deborah A. DeMott, *Relationships of Trust and Confidence in the Workplace*, 100 CORNELL L. REV. 1255, 1261 (2015) (finding that "courts impose ad hoc or fact-based fiduciary duties when although the parties' relationship was not categorically fiduciary, its characteristics nonetheless justified one party's expectation of loyal conduct from the other").

these justifications across the sweep of the relationship.[286] But the designation applies even more accurately with respect to employee data.

The notion of information fiduciaries has a somewhat hoary provenance but is also a relative recent policy innovation.[287] Like other fiduciaries, the information fiduciary has special responsibilities to individuals for whom the fiduciary holds or controls something of special value. But in this case, the thing of special value is information.[288] Many professionals who keep their clients' information confidential, such as doctors and lawyers, are essentially information fiduciaries in the course of their relationship with their clients.[289] Because these relationships involve the collection, analysis, use, and disclosure of sensitive information, the information fiduciaries must not use information obtained in the course of the relationship "in ways that harm or undermine the principal, patient, or client, or create conflicts of interest with the principal, patient, or client."[290]

Employers are an ideal match with the concept of information fiduciaries. The use of worker data is multifaceted: sometimes it is kept private from all but a few other employees; other times it is shared within the

---

[286] *See* Matthew T. Bodie, *Employment as Fiduciary Relationship*, 105 GEO. L.J. 819, 854-62 (2017).

[287] *See* Jack M. Balkin, *Information Fiduciaries in the Digital Age*, BALKINIZATION (Mar. 5, 2014, 4:50 PM), http://balkin.blogspot.com/2014/03/information-fiduciaries-in-digital-age.html (developing the idea of an "information fiduciary" and discussing how the concept is reflected in existing fiduciary law). *See also* Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497, 499 (2019) (discussing how Kenneth Laudon appears to have coined the term in 1990). For an alternative approach based on the duty of loyalty, see Neil Richards & Woodrow Hartzog, A Duty of Loyalty for Privacy Law, Working Paper, (July 3, 2020), https://ssrn.com/abstract=3642217 (setting out a theory of loyalty based upon "the risks of digital opportunism in information relationships").

[288] Balkin, *supra* note 281, at 1209 ("An information fiduciary is a person or business who, because of their relationship with another, has taken on special duties with respect to the information they obtain in the course of the relationship.").

[289] *Id.*

[290] *Id.* Interestingly, Balkin mentions vulnerability related to data collected by Uber—but he is concerned primarily not with employees, but with customers. *Id.* at 1187-91.

firm; and sometimes it is used by the firm in its relationships with suppliers, customers, and even society. The employer uses its discretion in processing this information; employees are vulnerable to the employer's use of the data and to potential opportunism; employees have trust and confidence in the employer to use the data appropriately; and the parties reasonably expect this to be the case. Employers exercise discretion over the employees' practical interests and critical resources—namely, their data.[291]

Some commentators have argued for a more contractual approach to information protection, noting that if parties want one party to have duties over the information, they can contract for confidentiality.[292] But if fiduciary duties could be handled purely by contract, we would have no need for them. Employees owe fiduciary duties to employers in addition to their contractual responsibilities because the employer cannot dictate every aspect of the job in the contract.[293] The relationship is similarly incomplete from the employees' perspective; with regard to employee data, the employer's use of that data cannot be reduced to specific contractual provisions at the outset of the relationship.[294] Given the resulting incompleteness, fiduciary duties are justified to balance out the expectations of the parties and prevent opportunism.[295] Moreover, individual employees lack the legal understanding and bargaining strength to negotiate for the appropriate level of protections.

---

[291] Smith, *supra* note 282, at 1402.

[292] Volokh, *supra* note 270, at 1051; *cf.* Larry E. Ribstein, *Fencing Fiduciary Duties*, 91 B.U. L. REV. 899, 900 (2011) ("[T]he fiduciary duty is most usefully viewed as a type of contract.").

[293] RESTATEMENT (THIRD) OF AGENCY § 1.01 cmt. g (AM. LAW INST. 2006) ("As agents, all employees owe duties of loyalty to their employers.").

[294] Stephen M. Bainbridge, *Participatory Management Within a Theory of the Firm*, 21 J. CORP. L. 657, 664 (1996) ("Because employees and employers cannot execute a complete contract under conditions of uncertainty and complexity, many decisions must be left for later contractual rewrites imposed by employer fiat."); Kent Greenfield, *The Place of Workers in Corporate Law*, 39 B.C. L. REV. 283, 317 (1998) ("Workers and management thus face significant barriers to contracting, in that they face huge transaction costs in reducing to writing all the implicit understandings necessary to reach the outcome best for both parties.").

[295] *See* Jordan v. Duff & Phelps, Inc., 815 F.2d 429, 438 (1987) ("Employment creates occasions for opportunism.").

Employee consent to the employers' terms—which often include duties of confidentiality, nonsolicitation agreements, and covenants not to compete—cannot be taken as a true indicia of the fairness of the underlying contract.[296]

The concept of an information fiduciary recognizes that "certain kinds of information constitute matters of private concern not because of their content, but because of the social relationships that produce them."[297] The exact nature of the duties imposed upon employers as information fiduciaries would be open to further development.[298] The critical notion would be one of protection: employers would be prohibited from using employee data to harm them opportunistically.[299] The relationship is a complicated one, and we should acknowledge that employees are "information fiduciaries" for the employer as well.[300] Fortunately for employers, an array of intellectual property protections, especially trade secret law, step in to protect them against unfair employee opportunism.[301] Workers need a counterbalance on the other side—a recognition of the responsibilities that their companies must accept as part of the employment relationship.

C. *Worker Participation in Informational Governance*

---

[296] The GDPR understands this power imbalance and will largely not see employee consent as sufficient to justify the processing of workplace data. GDPR, *supra* note 274, Art. 7; WP Work Opinion, *supra* note 276, at 6-7.

[297] Balkin, *supra* note 281, at 1205.

[298] *Cf.* Smith & Lee, *supra* note 282, at 635 (arguing that fiduciary duty should "distinguish the *appropriate pursuit of self-interest* from the *inappropriate pursuit of self-interest*" (emphasis in original)).

[299] RESTATEMENT (THIRD) OF AGENCY § 8.01 (AM. LAW INST. 2006) ("An agent has a fiduciary duty to act loyally for the principal's benefit in all matters connected with the agency relationship."); Balkin, *supra* note 281, at 1186 (fiduciaries should "act in ways that do not harm the interests" of those to who they owe fiduciary duties). Neil Richards and Woodrow Hartzog develop the concept of loyalty into a robust theory for data management. *See* Richards & Hartzog, *supra* note 287, at 6 (offering a theory "based on the risks of opportunism that arise when people trust others with their personal information and online experiences").

[300] *See, e.g.*, Andrew Frazier, *The Employee's Contractual Duty of Fidelity*, 131 L.Q. REV. 53, 54 (2015) (discussing opportunities for employee opportunism).

[301] *See* Part II.B. *supra*.

A third avenue for better managing employee data would be bringing employees into the decision-making processes of collecting and using the data. Under current law, employees without union representation lack legal mechanisms for participating in decision-making about how the employer actually uses their data. Business organizational law has been remarkably successful in separating employment from ownership.[302] Employees hand over their labor, good will, and personal capital to the firm, but then the firm—established as a corporation, partnership, or LLC—directs those assets to the ultimate benefit of the organization's voting public, who are generally equity investors.[303] The end result is that all other stakeholders, including employees, are fenced out from participation in governance.[304]

Unions have the power to negotiate on behalf of workers about terms and conditions of employment, which includes the collection and use of employee data.[305] There is evidence that labor organizations are working with employers to manage the flow of information from employees, install appropriate protections for private data, and share the value created by the use of the data.[306] Professional athletes in the four major U.S. sports leagues

---

[302] *See* Dalia Tsuk, *Corporations Without Labor: The Politics of Progressive Corporate Law,* 151 U. PA. L. REV. 1861, 1864 (2003) (exploring "how, in the course of the twentieth century, legal scholars and political theorists helped remove the interests of workers (as differentiated from shareholders, officers, and directors) from the core concerns of corporate law and theory").

[303] Honorable Leo E. Strine, Jr., *The Dangers of Denial: The Need for A Clear-Eyed Understanding of the Power and Accountability Structure Established by the Delaware General Corporation Law*, 50 WAKE FOREST L. REV. 761, 766 (2015) ("In the corporate republic, no constituency other than stockholders is given any power.").

[304] *See* Brett H. McDonnell, *Employee Primacy, or Economics Meets Civic Republicanism at Work*, 13 STAN. J.L. BUS. & FIN. 334, 335 (2008) (arguing instead for employee primacy in corporate decision-making).

[305] 29 U.S.C. §§ 158(a)(5), 8(d) (providing for the duty to bargain in good faith). Although data collection would generally fall into the terms and conditions category, data use could be considered part of the business operations and therefore left to the "core of entrepreneurial control." *See* Fibreboard Paper Prods. Corp. v. NLRB, 379 U.S. 203, 223 (1964) (Stewart, J., concurring).

[306] Lisa Kresge, Union Collective Bargaining Agreement Strategies in Response to Technology, Working Paper, Nov. 2020, https://laborcenter.berkeley.edu/wp-

are all unionized and, as discussed earlier, have complex systems of information management as part of their collective bargaining agreements.[307] For most employees, however, collective bargaining is not a viable option for information management.[308] Just over one in ten employees is represented by a labor organization, and only 6.2% of private sector employees are unionized.[309]

No doubt the many roadblocks to collective bargaining should be lifted.[310] But there are a plethora of potential organizational structures that could facilitate worker participation in actual governance, both as a general matter and specific to workplace data management. The system of corporate codetermination, required in many countries but most well-known in its German version, requires that employees at large companies choose fifty percent of the company's supervisory board.[311] Codetermination facilitates employee voice at the highest levels of power and would allow employees to push the board for better data relationships[312] Recently two bills have

---

content/uploads/2020/12/Working-Paper-Union-Collective-Bargaining-Agreement-Strategies-in-Response-to-Technology.pdf.

[307] *See* Part III.C *supra*.

[308] For a discussion of the causes of the low rate of unionization, see Cynthia L. Estlund, *The Ossification of American Labor Law*, 102 COLUM. L. REV. 1527 (2002).

[309] BUREAU OF LABOR STATISTICS, UNION STATISTICS – 2020, Jan. 20, 2021, https://www.bls.gov/news.release/pdf/union2.pdf

[310] *See, e.g.*, Protecting the Right to Organize ("PRO") Act, H.R. 2472, 116th Cong. § 2(c) (2020). For a proposal to modernize the NLRA's purpose of equal bargaining power through innovative social scientific analysis, see Hiba Hafiz, *Structural Labor Rights*, 119 MICH. L. REV. 651 (2021).

[311] Katharina Pistor, *Codetermination: A Sociopolitical Model with Governance Externalities*, in EMPLOYEES AND CORPORATE GOVERNANCE 163, 174-75 (Margaret M. Blair & Mark J. Roe eds., 1999). The fifty-percent requirement applies to companies with more than 2000 employees. Companies with between 500 and 2000 employees must have 30% employee representation on the supervisory board. *See* Otto Sandrock & Jean J. du Plessis, *The German System of Supervisory Codetermination by Employees*, in GERMAN CORPORATE GOVERNANCE IN INTERNATIONAL AND EUROPEAN CONTEXT (Jean J. du Plessis et al. eds., 2012).

[312] For a discussion of an American approach to employee governance participation, including codetermination, see GRANT M. HAYDEN & MATTHEW T. BODIE,

proposed American versions of codetermination, making it less fanciful an idea than in the past.[313]

But codetermination is by no means the only model. Industries with high levels of worker data management could reorient their organizational structures to facilitate employee ownership. Gig workers, for example, could own the platforms upon which they work through a workers' cooperative or nonprofit association.[314] Others have suggested management-labor coordination models, such as a hiring hall.[315] There are also internal governance mechanisms that facilitate employee involvement. With labels such as "self-managed," "self-actualizing," and "evolutionary,"[316] new models of participatory management work within the organizational structure to give workers power over their workplace.[317] Although these systems generally lie

---

RECONSTRUCTING THE CORPORATION: FROM SHAREHOLDER PRIMACY TO SHARED GOVERNANCE 172-83 (2021).

[313] The Accountable Capitalism Act, proposed by Senator (and former presidential candidate) Elizabeth Warren would require that companies with more than $1 billion in average revenue have employees select at least 40% of the seats on the board. Accountable Capitalism Act, S. 3348, 115th Cong. (2018). Senator Tammy Baldwin has proposed the Reward Work Act, which proposes that one-third of directors be selected directly by employees. Reward Work Act, S. 2605, 115th Cong. (2018).

[314] *See* Veena Dubal & Sushil Jacob, *Escaping the Wage-Slave/Micro-Entrepreneur Binary: Platforms for Liberating Labor*, J. AFFORDABLE HOUSING & COMMUNITY DEV. L., 2017, at 67 (proposing "an online marketplace that is owned and democratically governed by its members"); Ariana R. Levinson, *Founding Worker Cooperatives: Social Movement Theory and the Law*, 14 NEV. L.J. 322 (2014).

[315] *Cf.* Sanjukta M. Paul, *Uber As for-Profit Hiring Hall: A Price-Fixing Paradox and Its Implications*, 38 BERKELEY J. EMP. & LAB. L. 233, 253 (2017) (suggesting that "the difference between a hiring hall and Uber lies only in the distribution of the premium from price coordination that both engage in").

[316] *See* FREDERIC LALOUX, REINVENTING ORGANIZATIONS: A GUIDE TO CREATING ORGANIZATIONS INSPIRED BY THE NEXT STAGE OF HUMAN CONSCIOUSNESS 43 (2014) (using "self-actualizing," "evolutionary," "integral," and "teal"); Ethan Bernstein et al., *Beyond the Holacracy Hype*, HARV. BUS. REV. 38, 40 (July–Aug. 2016) (using "self-managed" and "flat").

[317] One particular instantiation of this broader movement is a system known as "holacracy." *See, e.g.*, BRIAN J. ROBERTSON, HOLACRACY: THE NEW MANAGEMENT SYSTEM FOR A RAPIDLY CHANGING WORLD (2015).

outside formal legal structures, law could incentivize their adoption and remove existing barriers to their work.[318] We could also require works councils—firm-level or worksite-level organizations that consult with management on issues of day-to-day employment.[319] These councils have had significant success in managing workplace issues in Germany and other European countries.[320]

A wrinkle on the works council more specific to the issue of workplace data would be a "data council." The law could require employers to implement a committee of workers and management to review and approve any collection or use of employee data. Data councils could also be tasked with creating an "employee data privacy policy," which—like consumer data privacy policies—could render the employer liable in the event that the policy was violated.[321] Creation of a data council and deference to its determinations could alternatively act as a safe harbor against employee claims of privacy intrusion and data confiscation.[322]

Each of these different proposals has its own strengths and weaknesses, its own scope and parameters. The important thread running through them is the ability of workers to participate collectively in the management of their collective data. The economic firm and its legal instantiations are meant to facilitate the process of joint production. In the process, they have facilitated the capture of employee data. Workers need to assert collective power to protect their private data, insure that they receive the benefits of that data, and carve out spaces for entrepreneurial opportunities and autonomy.

---

[318] There is some concern that the NLRA's prohibition on company unions might prohibit certain forms of employee participation in the absence of a union. Matthew T. Bodie, *Holacracy and the Law*, 42 DEL. J. CORP. L. 619, 662-71 (2018).

[319] Stephen F. Befort, *A New Voice for the Workplace: A Proposal for an American Works Councils Act*, 69 MO. L. REV. 607 (2004).

[320] *Id.* at 609-10.

[321] Violations of the policy could be considered breach of contract or a deceptive practice akin to those regulated by the Federal Trade Commission under § 5 of the FTC Act. *Cf.* 15 U.S.C. § 45.

[322] Tech companies are now exploring the use of oversight boards to manage constituency concerns and provide for more democratic resolutions. *See* Kate Klonick, *The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression*, 129 YALE L.J. 2418 (2020).

CONCLUSION

The novel coronavirus pandemic provides a stark example of the need to reexamine the regulation of workplace data. In the absence of an OSHA regulatory response,[323] businesses struggled to find the appropriate response to questions about when to reopen, appropriate safety measures, and the degree of risk that is acceptable for workers to shoulder. Workers have been asked to share their temperatures, health conditions, and test results with their employers to prevent spread of the disease.[324] Contact tracing apps follow employees at work and at home to monitor their interactions.[325] If employers put these information-sharing burdens on employees without providing for their participation, these policies will exacerbate employees' feelings of powerlessness, alienation, and violation. Participation, on the other hand, will provide workers with the opportunity to balance their privacy interests against concerns about contagion and infection. Employers and employees need not have oppositional interests here, but workers can be justifiably suspicious.[326] Participation can counteract actual and imagined employer opportunism.

---

[323] OSHA has provided only permissive guidance. OSHA, Protecting Workers: Guidance on Mitigating and Preventing the Spread of COVID-19 in the Workplace, https://www.osha.gov/coronavirus/safework (last visited Feb. 21, 2021).

[324] Natasha Singer, *Employers Rush to Adopt Virus Screening. The Tools May Not Help Much.,* N.Y. TIMES (May 11, 2020), https://www.nytimes.com/2020/05/11/technology/coronavirus-worker-testing-privacy.html.

[325] Kif Leswing, *As Workplaces Slowly Reopen, Tech Companies Smell a New Multibillion-Dollar Opportunity: Helping Businesses Trace Coronavirus*, CNBC.COM (May 10, 2020), https://www.cnbc.com/2020/05/10/coronavirus-tracing-for-workplaces-could-become-new-tech-opportunity.html.

[326] Nicole Dungca, Jenn Abelson, Abha Bhattarai & Meryl Kornfield, *On the Front Lines of the Pandemic, Grocery Workers are in the Dark about Risks*, WASH. POST (May 24, 2020), https://www.washingtonpost.com/investigations/2020/05/24/grocery-workers-coronavirus-risks/

The law relating to the collection and use of employee data needs a reconceptualization. The existing patchwork of privacy laws provides uncertain relief, and intellectual property laws largely hand ownership over the firm. The law has encased employer power over employee data through these limited privacy protections and expanding intellectual property allotments.[327] We need a system that will recognize ongoing employee interests in their data, that will make employers accountable for their stewardship of this data, and that will give workers power and control over this information within the firm. By recognizing worker data rights in a variety of contexts and forms, we can empower employees within their workplaces and ameliorate the dehumanizing disconnections of modern labor.

[327] *See* Kapczynski, *supra* note 265, at 1508-14 (discussing how law encases the power of information capitalists).