The Law of Employee Data: Privacy, Property, Governance

Matthew T. Bodie
Saint Louis University, matthew.bodie@slu.edu

Follow this and additional works at: https://www.repository.law.indiana.edu/ilj

Part of the Intellectual Property Law Commons, Labor and Employment Law Commons, Privacy Law Commons, and the Property Law and Real Estate Commons

Recommended Citation
Available at: https://www.repository.law.indiana.edu/ilj/vol97/iss2/7

This Article is brought to you for free and open access by the Maurer Law Journals at Digital Repository @ Maurer Law. It has been accepted for inclusion in Indiana Law Journal by an authorized editor of Digital Repository @ Maurer Law. For more information, please contact kdcogswe@indiana.edu.
The Law of Employee Data: Privacy, Property, Governance

MATTHEW T. BODIE*

The availability of data related to the employment relationship has ballooned into an unruly mass of performance metrics, personal characteristics, 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. My appreciation to the staff of the Indiana Law Journal, especially Preston Michelson, for their excellent editorial work. I am much obliged for research assistance from Danielle Durban, Andrew Keady, and Michael McMahon.
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). Over 600,000 emails within the Corpus were sent or received by 158 Enron executives through their employer’s Microsoft Outlook database. FERC seized the database as part of its investigation into 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.

In its original state, the Corpus was an 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. The dataset has since become fodder for over 100 research projects and commercial applications in computer science, with its most influential uses in the realm of artificial intelligence. Using these emails as raw data for real, person-to-person conversations, AI systems from Apple’s Siri to Google’s “smart compose” feature developed their

5. Purtill, supra note 2.
6. Id.; Heller, supra note 4.
understanding of speech based on this set of communications among Enron employees.\(^7\)

The story of the Enron Corpus raises many issues. 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.\(^8\) 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 troubled culture was embedded in machine learning systems.\(^9\) The use of the Corpus represents another instance of AI systems learning from flawed and biased examples to reproduce inequality.\(^10\)

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.\(^11\) Abruptly to light came personal details such as complaints from the CEO’s daughter about wedding invitations and a heretofore undiscovered office tryst.\(^12\) The dataset was redacted on several occasions to protect personal information, but even mundane emails inevitably exposed the authors to unexpected scrutiny.\(^13\) 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.

Along with these concerns, however, 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 to make great leaps in artificial intelligence. Simply by going about their daily business within the company, Enron employees developed a connected 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

---


8. See 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.”).

9. 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.”).


12. Id. at 648–49; Leber, supra note 7.

recorded human conversation. But this data is almost never made publicly available. The Enron Corpus is thus something of a unicorn—a set of real business communications that were made available to all and do not have meaningful copyright, privacy, or trade secret protections that might otherwise entangle researchers in legal claims. The 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 information into valuable fuel. Data 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.” 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. We have paid insufficient attention to data within and from employment.

We generally regulate worker data under two legal categories: privacy and intellectual property. Privacy laws are invoked to shield workers’ personal information in specific places and contexts, such as lockers, drug tests, genetic histories, and credit scores. On the other hand, intellectual property law generally hands employment-related data over to the employer through legal mechanisms such as trade secrets or copyright’s “work-for-hire” doctrine. 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’

14. Levendowski, supra note 9, 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 7 (“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.”).


16. Sam Adler-Bell & Michelle Miller, The Datafication of Employment, CENTURY FOUND. (Dec. 19, 2018), https://tcf.org/content/report/datafication-employment-surveillance-capitalism-shaping-workers-futures-without-knowledge/?agreed=1 [https://perma.cc/CLK9-MHMQ (“For consumers, the digital age presents a devil’s bargain . . . . But less well understood is the way data—in its collection, aggregation, and use—is changing the balance of power in the workplace.”)).

17. This Article uses “employee data,” “worker data,” and “work-life 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.

temperatures, impose requirements over personal health choices, and monitor those who are working from home. Workers are finding themselves virtually enmeshed within their businesses—without control, ownership, or regulatory protection.

In response to this increasingly fraught set of dynamics, advocates and academics have generally proposed a ratcheting-up of workplace privacy protections. 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, law should empower employees with respect to their data across a variety of contexts. That empowerment is grounded within concepts of privacy, intellectual property, and governance to strengthen the bonds between worker and data. This multidimensional approach is necessary to manage the role of data in myriad aspects of the employment relationship. Moreover, it reflects the successful methods deployed by workers in relative positions of power who 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 through privacy and intellectual property regimes. 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 individual employees within the economic firm. The Article then compares the data relationship that firms have with less empowered workers, such as platform drivers, with more empowered workers—specifically, professional athletes. Finally, in Part IV, the Article proposes a new framework for regulating worker data: outfitting employees with continuing but nuanced 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 as an individual—on the job or off—as well as the work done by the employee. It is any information generated by the employee. Sometimes that information is seen as distinctly personal, as in the employee’s weight, chronic illnesses, or political leanings, but it also includes information that the employee generates within the scope of employment, such as the calls that the salesperson makes to customers, the path of movements tracked by GPS, and gossip exchanged between coworkers.21 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 marker of employee data is that it derives from a particular person—an individual employee—but it is not confined to “personal” information.22

Collecting and using data about workers is endemic to employment relationships throughout history.23 Frederick Taylor based his system of scientific management on direct observation of workers in the process of working.24 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.25 But this

21. 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 (Oct. 15, 2017, 8:49 AM), https://www.usatoday.com/story/tech/talkingtech/2017/08/01/wisconsin-employees-got-embedded-chips/529198001/ [https://perma.cc/RV6M-J5ZD].

22. 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).

23. See, e.g., Ajunwa, Crawford & Schultz, supra note 20, 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, 217 (2017) (“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.”).

24. 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 W. 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, Richard A. Beaumont & Roy B. Helfgott eds., 2003).

25. BRUCE E. KAUFMAN, THE ORIGINS & EVOLUTION OF THE FIELD OF INDUSTRIAL RELATIONS IN THE UNITED STATES 24 (1993); see also GORDON S. WATKINS, AN
change also meant an expansion of the relevant zone of information—an expansion to include the worker’s personality and desires. Henry Ford, an early practitioner of personnel management, created a “Sociological Department” to delve into workers’ personal lives. The company hired a team of 150 investigators to survey workers’ personal habits, such as smoking, drinking, and gambling, as well as their spending and saving practices. As it developed into a field of study, personnel management (later called human resources management) grew to include the use of psychological tests, organizational dynamics, and even the effects of monitoring itself.

The last twenty 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. And its influence extends to all corners of our lives, from dating apps to traffic-displaying maps to recommended prison sentences. Big Data in the employment relationship—sometimes referred to as “people analytics”—has created a new data-driven approach to human resources management.

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

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.”).


27. Samuel M. Levin, Ford Profit Sharing, 1914–1920: 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.”).


32. ZUBOFF, supra note 15, at 138–55 (discussing the “dispossession” cycle of consumer data).


make workplace decisions. Technological advances have enabled employers to collect almost infinitely more data from their workers. 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. Video and audio recordings are now created digitally, making them significantly easier to record and store. Other electronic devices record employee movement, browser history, heart rate, temperature, and interactions with other employees.

To match up with this massive influx of data, employers have new ways of analyzing it. 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, these analytics tools can work through the numbers to find unexpected correlations. As one example, Google applies its own brand of data analytics to its human resources department, which it calls “People Operations.” Among the unusual approaches that Google has taken: paying talented workers substantially 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. For its “Project Aristotle,” an internal initiative to study the metrics of success among Google teams, the company intensively surveyed workers during group projects to understand what factors created a top team.

As the data collected in this new environment has become increasingly individualized, the line between person as individual and person as employee has become significantly blurred. The SARS-CoV-2 pandemic only exacerbated this
trend. Long considered to be particularly private information, employee health status became newly relevant to workplace operations. Employers took their workers’ temperatures, administered novel coronavirus tests, and managed the news of an employee’s positive test with other workers and medical professionals. As the Delta variant took hold, many employers imposed vaccine requirements on employees or asked unvaccinated employees to undergo rigorous protocols for the protection of coworkers and customers. Health information and decisions that were once considered purely personal have become subject to employer review.

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 hated being around kids. In these cases, what employees considered to be private became very public through the internet and social media, and ultimately these situations affected the reputation of their employers. Information about one employee can change the valuation of a company, the arc of its business model, and 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. But even frontline workers can have an impact on the reputation of the company.

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.”).


45. Bodie & McMahon, supra note 19, at 54–58.


49. 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
oriented businesses, the work of individual employees is the key to building the value of the brand.\textsuperscript{50} 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.\textsuperscript{51} And information about what they do in their off time now has much broader ramifications.

In a growing number of employment relationships, employee-generated data constitutes, in whole or in part, the output of the employer itself.\textsuperscript{52} To take but a few examples—doctors give medical advice and prescribe medicine, lawyers provide legal counsel and advocacy, and media companies publish their workers’ missives. We understand this more intuitively when it comes to formal intellectual property: copyrights become the property of the business entity through the “work-for-hire” doctrine, and most employee patents are assigned to the company as part of the employment agreement.\textsuperscript{53} But slippery sets of information have been enfolded into trade secret law, covering wider swaths of 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.\textsuperscript{54} 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.\textsuperscript{55} And that data is often provided by workers. Uber and Lyft, for example, track their drivers as part of a huge algorithm of traffic and transportation that has significant independent value.\textsuperscript{56} There is even evidence that some companies may be profiting from their employees’ data through sales to third parties.\textsuperscript{57}


\textsuperscript{50} See, e.g., \textsc{Tony Hsieh}, \textit{Delivering Happiness: A Path to Profits, Passion, and Purpose} 142–46 (2010).


\textsuperscript{52} See \textsc{Jeremias Prassl}, \textit{Humans as a Service: The Promise and Perils of Work in the Gig Economy} 54–55 (2018).

\textsuperscript{53} See infra Part II.B.

\textsuperscript{54} \textsc{Unif. Trade Secrets Act} § 1(4) (amended 1985), 14 U.L.A. 538 (2005).


\textsuperscript{57} Adler-Bell & Miller, supra note 16 (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”).
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 enterprise. Nothing seems to be off the table. In this world of employee embeddedness within an immersive world of data, how will law react through 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 property. These two different legal regimes together create the topography from which employees and employers operate.

A. Employee Privacy Protections

No comprehensive U.S. privacy law protects employees’ information. Instead, we have a loose network of provisions, ranging from constitutional law to common law to statutory law, many of which apply in a variety of contexts. The U.S. Constitution prohibits unreasonable searches and seizures under the Fourth Amendment and potentially extends a federal right of information privacy—as yet


not fully decided. These protections apply to average citizens as citizens but only apply to public-sector employees in the context of employment.

The common law offers wider-ranging protection. The tort of intrusion upon seclusion 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.” Courts have found the potential for liability in a variety of workplace situations, such as when an employer spied on an employee to get information for a workers’ compensation claim, when “fake” employees were dispersed into the workforce to get private information about fellow workers, when lockers were searched without consent, and when cameras were installed in bathrooms or private offices. The Restatement of Employment Law specifies that the tort applies in the employment context to protect the physical person, physical and electronic locations, and personal information. 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.

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 provides some protection against collection and intrusion in extreme cases. But there is no federal or state


63. 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.”).

64. Restatement (Second) of Torts § 652B (Am. L. Inst. 1977). The California Supreme Court has analogized the California constitutional protections to the privacy tort of intrusion upon seclusion. 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. Compare id. § 7.05, with Restatement (Second) of Torts § 652D (Am. L. Inst. 1977).

71. See, e.g., 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 Ctr. v. Superior Ct., 61 Cal. Rptr. 2d 187, 195 ( Ct. App. 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”).
law generally protecting the privacy of information related to employee health. Many believe the federal Health Information Portability and Accountability Act (HIPAA)\(^2\) shields health data, but HIPAA only applies to health plans, health care providers, and health care clearinghouses.\(^3\) Employers are not covered unless they provide health care or self-administered health insurance coverage.\(^4\) And even covered entities need not comply with HIPAA as to employment records when held in their role as employer.\(^5\)

Other regimes cover limited aspects of the employment relationship. The Americans with Disabilities Act (ADA) bars certain inquiries and examinations that would reveal employee disabilities or other health conditions.\(^6\) Wisconsin employers cannot ask their employees about HIV status.\(^7\) The Genetic Information Nondisclosure Act (GINA)\(^8\) was originally passed to protect against discrimination based on the results of genetic testing,\(^9\) but it has taken on a separate role prohibiting companies from snooping around in employees’ genetic data.\(^10\) Statutes in roughly three-quarters of the states also protect genetic information in employment, but these have had an “extremely limited impact.”\(^11\) The notable standout is Illinois’s Biometric Information Privacy Act (BIPA), which provides a private right of action


\(^{3}\) 45 C.F.R. § 160.103 (2020) (defining “covered entity” as a health plan, a health care clearinghouse, or a health care provider).

\(^{4}\) 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.”).

\(^{5}\) 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) (stating that, 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.).

\(^{6}\) See 42 U.S.C. § 12112(d). The Seventh Circuit has held that an employer’s administration of the Minnesota Multiphasic Personality Inventory (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, 837 (7th Cir. 2005).


\(^{9}\) 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”).


\(^{11}\) Areheart & Roberts, supra note 80, at 763.
for improper collection, retention, or use of biometric data. Workers have brought claims under BIPA regarding the use of their biometric data without sufficient disclosure, consent, and security protections. Finally, states have a variety of statutory and common-law regulations of employee drug testing while generally permitting it.

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. 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.” 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. With respect to information about prior arrests or convictions, state and local legislation prohibits employers from using that information at certain points in the hiring process.

When it comes to workplace surveillance, employers are allowed to monitor workers largely as they wish; even continual electronic observation is permitted. The common law forbids spying into the employee’s home, but it’s okay to watch the worker from a public vantage. Under federal law, an employer cannot intercept


87. 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.”).


89. See Ajunwa, Crawford & Schultz, supra note 20, 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, 181–82 (1st Cir. 1997) (permitting the use of cameras to continually survey the employees’ work space).

an employee’s telephone or other electronic communications, even from the employer’s phone, without specific consent. Hidden surveillance can be legally problematic if undisclosed, but secrecy is mostly permissible for significant and legitimate business reasons, such as to catch a thief. The National Labor Relations Act prohibits employer surveillance that would chill or otherwise interfere with its employees’ protected concerted activity. But beyond these examples there is no overall 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 employer interrogation, courts have looked primarily to the type of information being collected, viewing more favorably data collection that is job-related, skill-related, or qualification-related. Personality testing has long been an HR staple and is not usually problematic when mainstream tests are used. While questions on personality traits and emotional

proceedings on intrusion claim when the employer’s investigator secretly videotaped an employee in his home after gaining entry on false pretenses, with I.C.U. Investigations, Inc. v. Jones, 780 So. 2d 685, 689–90 (Ala. 2000) (no intrusion when videotaped in front yard); York v. Gen. Elec. Co., 759 N.E.2d 865, 866, 868 (Ohio Ct. App. 2001) (no intrusion when employer representative observed the employee arriving at work, going into his chiropractor’s office, visiting a lawn mower repair shop, mowing his lawn, and riding a motorcycle).

91. See 18 U.S.C § 2511 (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 & Co., 704 F.2d 577, 581–82 (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 . . . .”).


93. See 29 U.S.C. § 158(a)(1); see also 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”).

94. W. PAGE KEETON, DAN B. DOBBS, ROBERT E. KEETON & DAVID G. OWEN, PROSSER AND KEETON ON THE LAW OF TORTS § 117, at 121 (5th ed. Supp. 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.”).


96. The Minnesota Multiphasic Personality Inventory (MMPI), the Meyers-Briggs Type
intelligence are viewed as job related, examinations that look beyond those elements and into confidential or demographic information may be on more shaky legal ground. The federal Employee Polygraph Protection Act, along with a number of related state statutes, severely restricts the use of polygraph tests in collecting employee biometric data in response to substantive questions. Recently enacted state legislation prohibits employers from requesting access to personal social media accounts.

Once data has been collected from workers, employers are generally able to use that data as they wish. Data aggregation can reveal much more about employees than one might expect. Such aggregation can feel disturbing, even threatening, to

---

97. See Soroka v. Dayton Hudson Corp., 1 Cal. Rptr. 2d 77, 79–80 (Ct. App. 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”), review granted, 822 P.2d 1327 (Cal. 1992), review dismissed as moot, 862 P.2d 148 (Cal. 1993).


100. 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.”).

101. 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 Companies Learn Your Secrets, N.Y. TIMES MAG. (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html [https://perma.cc/89D5-QMZ4]. Employers have successfully developed similar profiles. Valentina Zarya, Employers Are Quietly Using Big Data to Track Employee Pregnancies, FORBES (Feb. 17, 2016, 5:36 PM), http://fortune.com/2016/02/17/castlight-pregnancy-data/ [https://perma.cc/27Q6-GBKE].
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 to the purpose for which it was collected, or to ensure the accuracy of the data.  

There are restrictions on disclosure. Under the “public disclosure of private facts” tort, an employer may be liable if it gives publicity to personal worker information. The duty of confidentiality generally arises from implicit or explicit promises, fiduciary relationships, specific statutory or regulatory requirements, or ethical rules or codes, and these may apply in certain employment relationships. But employers are generally not considered to be fiduciaries of their employees’ data unless they have specifically assumed that duty.

Employees’ privacy interests may also be infringed when employers allow their data to be accessed through faulty or negligent security systems, and some statutes
do impose security requirements on certain types of information. 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. Employee plaintiffs alleged that Sony’s inadequate security measures allowed the hack to take place, and the case was ultimately settled. However, other employee claims related to unintentional disclosures have not been successful. All fifty states have data breach notification laws which would apply to employers when there is a data breach involving employee personal data.

The law has made efforts to protect employee data against employer collection or use. But these protections are spotty—clumps of regulation that leave a lot of open territory. Although certain statutes, such as BIPA, put in place mandatory disclosure, consent, and security regimes, most privacy regulation can be waived by employees in the course of their employment. In the context of at-will employment, such waivers may become a condition of continued work.

B. Property Rights in Employee Data

A traditional justification for property rights stems from the concept of the “fruits of one’s labor”—a person should own her creations. But when operating within the aegis of a firm, workers contribute their labor to the firm in exchange for

106. For example, HIPAA regulations require that covered entities “[p]rotect against any reasonably anticipated threats or hazards to the security or integrity” of protected health information, 45 C.F.R. § 164.306(a)(2) (2020).


111. John Locke, Two Treatises of Government 306 (P. Laslett rev. ed. 1963) (3d ed. 1698) (“Whatever 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 postrevolutionary 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 labor 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), reprinted in 4 LAWS OF NEW HAMPSHIRE 521 (Henry Harrison Metcalf ed., 1916)).
payment, contributing their labor to the collective enterprise.\footnote{112} Academics have cited to this process of joint or team production as the justification for the firm itself.\footnote{113} But in the process, property rights that were once assigned to the individual become group property—owned by the employing enterprise.

Intellectual property has largely followed this division of ownership in the context of employment, as property rights usually end up in the hands of the employer. Employee works are covered 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.\footnote{114} Such works may be created by individuals or groups.\footnote{115} 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.”\footnote{116} The Copyright Act of 1976 modified the doctrine to make the employer the author of any work made for hire unless expressly agreed otherwise.\footnote{117} The 1976 Act defines “work made for hire” as “a work prepared by an employee within the scope of his or her employment.”\footnote{118} This rule of ownership can only be altered by a signed, written document that expressly changes it.\footnote{119} So when employees draft a screenplay or develop a software program in the context of employment, their employer owns the copyright.\footnote{120}

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.”\footnote{121} Because patent law looks to a human inventor as the recipient of the patent rights, the

\footnote{112} 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.”).

\footnote{113} 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).

\footnote{114} 17 U.S.C. § 102.

\footnote{115} See Anthony J. Casey & Andres Sawicki, Copyright in Teams, 80 U. CHI. L. REV. 1683, 1685 (2013) (discussing the collaborative production of copyrightable material).


\footnote{117} 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.”).

\footnote{118} Id. § 101.

\footnote{119} Id. § 201(b).

\footnote{120} 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).

\footnote{121} 35 U.S.C. § 101.
employee who invents the patent is the author.\textsuperscript{122} However, employers are free to contract with employees for the rights to all inventions created within the scope of employment. Even without an express 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.\textsuperscript{123} In addition, under the shop-right doctrine, employers enjoy a nonexclusive right to use the patent without having to compensate the employee. A shop right arises when the employee has created the invention on the job using the employer’s materials.\textsuperscript{124}

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 IP law and contracts, over the ideas and creations of their employees.\textsuperscript{125} 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.\textsuperscript{126} 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.\textsuperscript{127} But the scope of the “scope of employment” remains up for grabs.

\begin{footnotesize}
\begin{enumerate}
\item The patent must be registered by the individual inventor. See 35 U.S.C. §§ 111, 115 (discussing oath taken as part of patent process that the registrant is the “original and first inventor”).
\item 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.”).
\item FISK, supra note 123, at 118; Burk, supra note 123, at 16.
\item See id. at 797–803 (discussing examples involving a computer algorithm and a design for a new toy line).
\item 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
\end{enumerate}
\end{footnotesize}
Trade secrets have grown in importance under the Big Data economy. Protected through the common law, state statutes, and the federal Defend Trade Secrets Act, 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. Trade secrets can be almost any type of business information: a formula, pattern, compilation, program, device, method, technique, or process. The law prohibits an individual’s personal or professional skills from counting as a firm’s trade secrets, but commentators fear that a combination of trade secret expansion and contractual provisions will sweep up employees’ informational capital into the employer’s domain. Employees are generally presumed to have an implied duty to keep any trade secrets to which they are exposed confidential. Moreover, a few jurisdictions have applied the doctrine 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. A 2010 study of trade secret copyright infringement is exceedingly remote.

Levendowski, supra note 9, at 610–11 (footnote omitted).


132. See, e.g., Lobel, supra note 125.

133. See Unistar Corp. v. Child, 415 So. 2d 733, 734 (Fla. Dist. 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 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 125, at 810.

134. See, e.g., PepsiCo, Inc. v. Redmon, 54 F.3d 1262, 1269 (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
litigation found that 85 percent of cases involved either current or former employees or business partners.\textsuperscript{135}

Trademarks allow producers of goods or services to identify themselves as the source of those goods or services, and to prevent others from doing so.\textsuperscript{136} One of the primary justifications for trademark is to allow consumers to understand where goods come from in an understandable and efficient manner.\textsuperscript{137} Just as patent and copyright protections allocate rights between employee and employer as to creative and useful works, trademark allocates rights as to goodwill and reputation.\textsuperscript{138} Trademarks transfer reputational assets to the firm and deprive individual employees of their ability to hold up the firm or exploit the firm’s trade dress separately.\textsuperscript{139} 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 continue to use the same mark.

The right of publicity has been characterized both as a right to privacy\textsuperscript{140} as well as a personal IP right—something akin to trademark for people.\textsuperscript{141} An individual can deploy the right to prevent others from using her persona—her name, image, likeness, or other indicia of identity—without consent.\textsuperscript{142} The justifications for the

\textsuperscript{135} David S. Almeling, Darin W. Snyder, Michael Sapoznikow, Whitney E. McCollum & Jill Weader, \textit{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.” \textit{Id}. However, owners were also “over 70% more likely to lose a motion to dismiss when they sued employees than business partners.” \textit{Id}.

\textsuperscript{136} 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”).

\textsuperscript{137} Mark P. McKenna, \textit{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.”).


\textsuperscript{139} \textit{Id}. at 376–79.

\textsuperscript{140} The right to publicity has its origins in tort law and was one of Dean Prosser’s original four privacy torts. \textit{RESTATEMENT (SECOND) OF TORTS § 652C} (AM. L. INST. 1977) (providing protection against the appropriation of one’s name or likeness); \textit{see} Eric E. Johnson, \textit{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.”).

\textsuperscript{141} Stacey L. Dogan & Mark A. Lemley, \textit{What the Right of Publicity Can Learn from Trademark Law}, 58 STAN. L. REV. 1161 (2006); \textit{see also} Barton Beebe, \textit{What Trademark Law Is Learning from the Right of Publicity}, 42 COLUM. J. L. & ARTS 389, 389 (2019) (arguing that trademark and publicity “are converging in many important ways, giving us the worst of both worlds”).

\textsuperscript{142} \textit{RESTATEMENT (SECOND) OF TORTS § 652C} (AM. L. INST. 1977) (“One who appropriates to his own use or benefit the name or likeness of another is subject to liability to
right generally involve the protection of investment—financial, emotional, or moral—in one’s reputation and identity. 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. As the right of publicity has drifted closer to a property right, workers who can assign their identities over to their employer might lose control over those identities. 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. Employers have also been more and more aggressive about asserting control over employee information through contract provisions such as covenants not to compete and nondisclosure agreements. 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-generated data, putting workers at risk for loss of control, displacement, and alienation.

III. CRUMBLING PARADIGMS IN THE REGULATION OF EMPLOYEE DATA

Even though U.S. law has taken a primarily laissez-faire approach to the collection and use of employee data, it has provided some limited protections through privacy rights and intellectual property. Ultimately, however, the underlying...
assumptions that frame these regulatory regimes have become unsettled. This Part
examines the collapse of two primary paradigms that had supported the legal
infrastructure: the separation of personal information from business-related
information and the ability of employees to separate themselves 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
divergent consequences of datafication for these 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 “life” while at home and another while in
the workplace.149 The dividing line between work and home has played an important
role in allowing employers fairly unlimited discretion over the workplace.150 But this
division rests on the shaky foundation that the work self can be separated from the
personal self.

The development of the data-based approach to human resources has highlighted
the potential benefits of data-driven inquiries, including probing into data that would
be considered personal. The “people analytics” phenomenon involves the search for
new pools of quantitative data that are correlated with business and employment
success.151 Much of that data can be gathered at the workplace. But employers are
now diving much deeper into the employee’s intimate physical and psychological
profile as well. As Henry Ford understood, employee health affects work
performance, and illness can infect coworkers.152 The ability to know about workers
on a personal level has exponentially expanded. Companies can track and collect
data on employee eye movements, heart rate, gait, speech patterns, and
temperature.153 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.154

149. See Naomi Schoenbaum, The Law of Intimate Work, 90 WASH. L. REV. 1167, 1174

dictatorship that “does not recognize a personal or private sphere of autonomy free from sanction”).

151. See Bodie, Cherry, McCormick & Tang, supra note 34, at 973.

https://www.nytimes.com/2021/02/17/magazine/wellness-apps.html [https://perma.cc/KY5S-
8V29] (noting that sick workers cost companies $575 billion in 2019 and likely significantly
more in 2020).

153. See supra Part I.

154. See Wortham, supra note 152 (discussing the attraction of workplace wellness
programs for employers).
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 workplace discipline or discharge. While critics bemoan the rise of “cancel culture,” social media has expanded public exposure to what were heretofore private thoughts across the board. When unpopular or offensive views become associated with the company by virtue of the employment connection, termination often follows. As a result, workers must consider the employment ramifications for almost any activity—including texts that could be screenshotted or activities that could be recorded on video and uploaded. Further complicating matters, 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. With shutdowns and quarantines at the outset of the pandemic, over fifty percent of workers found themselves working at home; by late 2020, those numbers had drifted down to about a third but remain higher than before. Using telework software allows employees to engage in their jobs but still

155. Bodie, supra note 47.
159. See Bodie, supra note 47 (discussing medical resident who was recorded on video mistreating an Uber driver).
160. Wortham, supra note 152 (“The distinction between work and everything else, already a blurry line for most Americans, got even blurrier.”).
leaves them in their homes. For those workers who must physically be present on the job, their health and the health of their coworkers have greater salience than ever. Many employers instituted testing, tracing, and disclosure programs and required employees to get vaccinated.\textsuperscript{162} Indeed, workers have a strong interest in reducing cross infection within their ranks.\textsuperscript{163}

This disintegration of the personal/business divide substantially weakens protections for worker data rights through privacy law and intellectual property law.\textsuperscript{164} To a significant extent, U.S. law protects privacy within employment by drawing a line between personal information and business-related information. And intellectual property rights within the workplace are assigned to the employer, while creations outside of work belong to the individual workers. If the line between work and home breaks down, then so do the privacy protections and workers’ IP rights.

The law already assumes that workers have little expectation of privacy while actually at work. Surveillance is presumed.\textsuperscript{165} 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.\textsuperscript{166} 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.\textsuperscript{167} There seem to be

\hspace{1cm}


\textsuperscript{164}. Ajunwa, Crawford & Schultz, supra note 20, 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.”).

\textsuperscript{165}. See, e.g., Vega-Rodriguez v. P.R. Tel. 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.”).

\textsuperscript{166}. Ajunwa, Crawford & Schultz, supra note 20, at 742–44.

\textsuperscript{167}. Tiffany May & Amy Chang Chien, Slouch or Slack Off, This “Smart” Office Chair Cushion Will Record It, N.Y. TIMES (Jan. 12, 2021), https://www.nytimes.com/2021/01/12/world/asia/china-office-cushion-surveillance.html [https://perma.cc/P67A-PY7P].
no limit to ways in which employers can monitor and collect data from their employees.\textsuperscript{168}

The law has endeavored to provide some space for personal privacy and autonomy in the workplace, but those efforts are growing increasingly quixotic. Tort law has protected employees against invasions into their persons, personal space, and personal effects.\textsuperscript{169} 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.\textsuperscript{170} Even offices can provide an expectation of privacy when the door is closed.\textsuperscript{171} 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 be impermissible to knowingly record personal phone calls by workers,\textsuperscript{172} 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.\textsuperscript{173} Even in those cases, use of visual technology—binoculars, telescopic lenses—to see beyond the ability of the human eye from a public area is generally forbidden.\textsuperscript{174} But what if the employer is invited into the home through an app or a laptop? Several states require employers to follow certain protocols when electronically monitoring their employees, but these primarily ask for notice or consent.\textsuperscript{175} Unlike other countries, there are no mandatory “turn off”

\begin{itemize}
\item \textsuperscript{168} Ajunwa, Crawford & Schultz, supra note 20, at 742–44.
\item \textsuperscript{169} Restatement of Emp. L. § 7.03(a) (Am. L. 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”).
\item \textsuperscript{170} Id. § 7.03 cmt. b.
\item \textsuperscript{171} E.g., Hernandez v. Hillsides, Inc., 211 P.3d 1063, 1075–76 (Cal. 2009).
\item \textsuperscript{172} See, e.g., Deal v. Spears, 980 F.2d 1153, 1158 (8th Cir. 1992) (finding that recording personal employee calls violated the Wiretap Act).
\item \textsuperscript{173} Restatement of Emp. L. § 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”).
\item \textsuperscript{174} Id. § 7.03 cmt. n, 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.”)
\item \textsuperscript{175} 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 (2021); see also Kendra Rosenberg, Note, 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. Cal. Civ. Code §§ 1798.145(h)(3), 1798.100 (2021). Connecticut requires employers to provide prior written notice of the monitoring. Conn. Gen. Stat. § 31-
or disconnect periods—employees can be asked to remain accessible regardless of
the hour.\textsuperscript{176} And under employment at will, employees can be terminated for their
off-duty conduct, with only limited protections for political or religious activity.\textsuperscript{177}

The personal/business divide is also critical to intellectual property law. The
Enron Corpus seems like it was once 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.”\textsuperscript{178} But those claims would only apply to the extent that these emails
were not written within the scope of employment, which would otherwise subsume
them into the employer’s property.\textsuperscript{179}

Like other areas of IP, 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. Anything
an employee may create that relates in some way to the worker’s job responsibilities
can become the employer’s property. Trade secrets also allocate ideas, concepts, and
data over to the employer’s side of the ledger.\textsuperscript{180} Hungry for power over even more
of their employees’ output, many companies have drafted broad assignment clauses
which bolster these existing doctrines through contract. In her book \textit{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.\textsuperscript{181} 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.”\textsuperscript{182}

\textsuperscript{176} Cf. French Workers Get 'Right to Disconnect' from Emails Out of Hours, BBC (Dec.
HM3N]; Katie Way, \textit{Workers of the World, Unplug: The Fight for the 'Right to Disconnect'},
VICE (Oct. 16, 2019, 2:10 PM), https://www.vice.com/en/article/evjk4w/right-to-disconnect-
legislation-labor-movement [https://perma.cc/6DPL-HJWU].

\textsuperscript{177} See Matthew T. Bodie, \textit{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); \textit{Restatement of Emp. L.} § 7.08
(AM. L. INST. 2015) (proposing a default contractual rule against termination for political and
ideological beliefs, or lawful conduct).

\textsuperscript{178} 17 U.S.C. § 102(a); see Levenskowski, \textit{supra} note 9, at 610.

\textsuperscript{179} See 17 U.S.C. § 201(b) (work-for-hire doctrine).

\textsuperscript{180} See Camilla A. Hrdy & Mark A. Lemley, \textit{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.”).

\textsuperscript{181} Orly Lobel, \textit{You Don’t Own ME: HOW MATTEL V. MGA ENTERTAINMENT EXPOSED
BARBIE’S DARK SIDE} (2017).

\textsuperscript{182} Id. at 22–24. The employee’s new company successfully showed that the designs had
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 distinctive 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 larger and more powerful entities. This diffusion of the individual into the collective is our second paradigm breakdown.

B. The Embeddedness of the Worker Within the Economic Firm

Much academic attention has focused on the fissuring of the economic firm.\textsuperscript{183} Advancements in technology, monitoring, and contracting have enabled firms to shed employees and instead to purchase labor through intermediaries.\textsuperscript{184} 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 selling rights to the brand to franchisees.\textsuperscript{185} These trends seem to signal the devolution of the firm and the weakening of its role in the economy.\textsuperscript{186} But fissuring instead provides an example of how firms can control and utilize workers while seeming to cut them loose. And data supplies the web that keeps these workers in place.

Fissuring can only happen when employers are still able to 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. Control over workers enables the firm to coordinate mass production while maintaining the integrity of the process. 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.’”\textsuperscript{187} 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.\textsuperscript{188} However, neither the legal scope of the firm nor the employer-employee relationship is critical if that direction and control can be exercised without them.

---

\textsuperscript{183} See, e.g., DAVID I. WEIL, THE FISSURED WORKPLACE: WHY WORK BECAME SO BAD FOR SO MANY AND WHAT CAN BE DONE TO IMPROVE IT (2014).

\textsuperscript{184} Rogers, supra note 18.

\textsuperscript{185} Id.


\textsuperscript{188} Id. at 404.
Our environment of data-rich communications and analytics enables fissuring to proceed apace.189 Firms need not hire employees if independent contractors can be nudged, adjusted, and directed by algorithms tracking their every move.190 Hotels can hire outside housekeeping contractors and yet still ensure that workers are providing high levels of service.191 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 not be considered the employer.192 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.193

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 massive transfer of power and wealth through the aggregation of data in the consumer context. Commentators have exposed the cycle of surveillance capitalism that profiles individual customers and then uses those profiles to target us for sales.194 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 than the traditional “notice and consent” approach.195 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.196 Portability allows users to change

189. Rogers, supra note 18, 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.”).
190. See MARY L. GRAY & SIDDHARTHI SURI, GHOST WORK: HOW TO STOP SILICON VALLEY FROM BUILDING A NEW GENERAL UNDERCLASS (2019) (discussing control exercised over platform-based workers).
191. WEIL, supra note 183, at 145–46.
193. 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 Airbnbss, Ubers, and eBays of the world”).
194. ZUBOFF, supra note 15.
196. CAL. CIV. CODE § 1798.100 (2021) (“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.”).
companies without losing the benefits of their accumulated data over time, whether that be posts, pictures, reputation scores, or performance metrics. Effectuating portability is easier in theory than in practice. But at least in the consumer context, efforts to empower consumers now address the embeddedness problem, rather than simply relying on notice and consent. 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 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. These assignments facilitate joint creation and distribution, but they swallow up individual contributions into an undifferentiated whole. 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. State and federal laws have reinforced the legal fortress around trade secrets while still not requiring that they be registered, identified, or even defined. As discussed earlier, workers are prohibited from taking such information with them and can even be enjoined from working elsewhere for fear of inevitable disclosure.

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.
Nondisclosure agreements can prevent the worker from sharing her personal experiences on the job, closing off an avenue of individual expression whether publicly or privately.\textsuperscript{205} Covenants not to compete 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.\textsuperscript{206}

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 govern a diverse set of contributors whose individual labors are difficult to compare or segregate.\textsuperscript{207} 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.”\textsuperscript{208} An independent monitor—the firm—would ensure that the team members all contribute appropriately and are then rewarded appropriately.\textsuperscript{209} 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.\textsuperscript{210}

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, 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 scenarios.

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.\textsuperscript{211} This despair is warranted considering the

\textsuperscript{205} Lobel, \textit{supra} note 199 (discussing how NDAs can expand “beyond the traditional categories of trade secrets, includ[ing] general know-how, client lists, and salary information”).

\textsuperscript{206} Lobel, \textit{supra} note 125, at 825–35.

\textsuperscript{207} Alchian & Demsetz, \textit{supra} note 113, at 777–78.

\textsuperscript{208} \textit{Id.} at 779.

\textsuperscript{209} \textit{Id.} at 782–83.

\textsuperscript{210} See Dan L. Burk & Brett H. McDonnell, \textit{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.”).

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.

Yes, most employers have 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. 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 passenger needs, enabling the platform to better attract drivers and riders. The process is all managed by sophisticated algorithms that feed on massive amounts of data.

Platform companies garner a vast trove of data from their workforce. They track location data to assign rides to drivers who are closest to customers. But along with tracking locations, the companies provide directions to drivers, and they track how effective those directions are over time. 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. 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. The companies also track other types of data about drivers, including reputation scores from customers, how long drivers are idle without engaging in a compensated ride, and even the physical

invasive technological surveillance has become”).

212. ALEX ROSENBLAT, UBERLAND: HOW ALGORITHMS ARE REWRITING THE RULES 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.”).

213. 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), https://time.com/5675637/uber-business-future/ [https://perma.cc/J3VQ-KLXJ] (“‘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.”).

214. ROSENBLAT, supra note 212, at 3 (“Rather than supervising its hundreds of thousands of drivers with human supervisors, the company has built a ride-hail platform on a system of algorithms that serves as a virtual ‘automated manager.’”).

215. Id.

216. Id. at 132–33.

217. Id. at 133.


219. ROSENBLAT, supra note 212, at 149–56.

stability of the phone within the car.\textsuperscript{221} Drivers must put their trust in the companies to manage this data, despite past failures in security.\textsuperscript{222}

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 drivers’ purview.\textsuperscript{223} Meanwhile, the platform companies use algorithms to manage drivers and provide only automated and inexpensive technical or managerial assistance.\textsuperscript{224} 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.\textsuperscript{225} In particular, they want data portability—a right under the GDPR—to obtain their data for their own purposes.\textsuperscript{226} 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.\textsuperscript{227} The Cooperative plans to aggregate, anonymize, and share the data with participating drivers.\textsuperscript{228} 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.\textsuperscript{229} The drivers are supplying the raw materials for this new automated system through their data—their labor—without any stake in its future success.

More data is likely collected from professional athletes than any other occupation. “People analytics” began in baseball in 1859 with the first box score.\textsuperscript{230} Ever since, professional athletes have been observed in every aspect of their performance on the

drivers-are-fighting-for-their-data [https://perma.cc/34UW-6T2B].

\textsuperscript{221} Rosenblat, supra note 212, at 141–42.

\textsuperscript{222} Id. at 163–64.

\textsuperscript{223} Holder, supra note 220 (quoting a driver as to his efforts to get his data to “assert my rights and eliminate the asymmetry in information power between me and Uber”).

\textsuperscript{224} Dan Lyons, Lab Rats: How Silicon Valley Made Work Miserable for the Rest of Us 150 (2018); Rosenblat, supra note 212, at 144.

\textsuperscript{225} Holder, supra note 220; Uber Drivers Demand Their Data, Economist (Mar. 20, 2019), https://www.economist.com/britain/2019/03/20/uber-drivers-demand-their-data [https://perma.cc/33AK-LGA2].

\textsuperscript{226} Holder, supra note 220.

\textsuperscript{227} Id.

\textsuperscript{228} Id.


The *Moneyball* phenomenon brought new sets of data and data analytics to the evaluation of players, and the search for untapped information continues apace. New statistics are constantly developed to capture all aspects of performance. And the search for metrics has long since moved beyond what happens on the court or field; monitoring now goes on twenty-four hours a day. The types of data are staggering: body and eye movements, elbow stress, skin temperature, heart rate, oxygen levels, glucose levels, hydration, and sleep rhythms. The avalanche of data techniques and analytics has led to the “hyperquantified athlete.”

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. But in looking at the bigger picture,
professional athletes have facilitated the use of their data in ways that inure to their benefit. 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. 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. Collective bargaining agreements in professional sports provide players with control and ownership over certain kinds of data. 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.

Even with their individual and collective market power, athletes are still pressing for stronger rights over their data. Many teams make participation in 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. In the United Kingdom, Project Red Card seeks to reclaim rights over player statistics in soccer from the many outside analysts and gambling agencies that process that data for their own economic benefit. These athletes claim that the GDPR renders the processing illegal without their consent.

Even with these concerns, however, 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. After all, the


240. See 29 U.S.C. § 158(a)(5) (setting forth the duty to bargain).

241. Busca, supra note 236.

242. Perhaps the most important publicity-rights case involved baseball cards. See Haelan Lab’y’s, Inc. v. Topps Chewing Gum, Inc., 202 F.2d 866 (2d Cir. 1953).


244. Hartley & Marsh, supra note 244 (“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 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.”).

purpose of these analytics is to improve the players’ performance, maximize playing ability, and prevent injury. 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 and analytics when 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 as well as the worker control and ownership over it. If workers can participate in the design of the data program, can object when it goes too far, and then can better themselves individually through the program, data analytics will be a positive development. These principles should guide us as we reimagine the legal regime of data regulation 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 efforts 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 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 nonpublic, personal data, such as health information, biometrics, personal communications, and political or religious beliefs. Such protections can also apply, albeit 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. 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.249 But these interests are not an either/or switch. Information that is traditionally considered personal may have value to the business, and creative expressions 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.

We need to blend these regimes because approaches based just on privacy rights or property rights would not work. A system constructed purely around privacy regulation fails to account for the unique features of the employment relationship. American privacy law focuses on the collection of information and imposes legal barriers to access when physical or electronic barriers fail.250 The traditional common-law intrusion tort largely imagines an invasion from the outside—a nonconsensual violation.251 But there are steady and significant flows of information between employers and employees covering a wide variety of subjects. Even the disclosure of extremely private information can at times be necessary.252 It is hard to find absolutes here.253 And it is inappropriate to borrow too much from consumer privacy regimes; although consumers may have ongoing data relationships, the information stream is generally not as thick and constant as between employee and employer. As a result, privacy protections will eventually become shredded, torn through by the many instances in which employers secure employee consent for collection, use, and disclosure.

As compared to privacy rights, property rights are meant to be more concrete and definable.254 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.255 In the context of the employment relationship, however, this move towards enclosure

249. 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. 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 CALIF. L. REV. 263, 300 (2009).
250. RESTATEMENT OF EMP. L. § 7.03 (AM. L. INST. 2015).
252. For an extreme example, see Feminist Women’s Health Ctr. v. Superior Ct., 61 Cal. Rptr. 2d 187 (Cal. App. 1997).
254. See, e.g., Bernstein, supra note 80, at 253 (“Privacy is considered a vague and protean concept.”).
creates difficulties for workers. 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 aggressively assert their rights over employee data and capture all of the economic value from this jointly contributed resource.

The strengths and weaknesses of the privacy and property approaches have become clear in the larger struggles over the management of personal data. Certain commentators have proposed a system of data property rights in order to give creators more control over the use of their data as well as an opportunity to participate in the value that their data creates. However, reception to this idea has largely been negative. Data property rights would further restrict the free flow of information, inhibiting the spread of knowledge and understanding. And if the property rights were alienable, personal data could easily come under the control of another—in our case, the employer. If inalienable, they would allow for the creation of an

256. See, e.g., Paul M. Schwartz, Property, Privacy, and Personal Data, 117 Harv. L. Rev. 2056, 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’Y 25, 34 (1999) (suggesting an intellectual property model for data privacy).


258. See Lothar Determann, No One Owns Data, 70 Hastings L.J. 1, 43 (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.”).

259. See Rothman, supra note 146, 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 property law favoring free alienability and information privacy policy preferences for restrictions on alienation.”).
anticommons.260 Any such regime would also raise significant logistical issues261 and free speech concerns.262

Separating out individualized data property cuts against the purpose of the firm—namely, to enable joint production. Firms facilitate productivity through joint production.263 The participants in 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 participants are all working together, they are treated as a unit under the law.264 The coordinating aspects of firm production allow for the whole to be greater than the sum of the parts.265

260. 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, 4 (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.").

261. Determann, supra note 258, at 5 ("[T]here is much uncertainty and ambiguity regarding the meaning of ‘data,’ ‘information,’ and ‘ownership’; little comprehensive analysis regarding how existing property laws already cover data or exclude data from protection; and relatively sparse considerations of legal and policy reasons for not granting property rights to data.").


264. Guy Davidov has recognized that the concept of employment 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).

265. Indeed, the data itself may be 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,
This unique informational relationship calls for a hybrid approach. The foundations of such an approach would have three characteristics. First, employees should 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). The rights include:

- 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).

These rights do not require “privacy” in the traditional American sense of fencing off certain information from access. Rather, they are rights to control the use of one’s data even after it is in another’s hands. These are exactly the kinds of rights 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 257, at 1499 (footnotes omitted).


267. GDPR, supra note 266, at arts. 5, 12, 15–17, 20.

268. The GDPR protects against inappropriate data collection through Article 6, which requires a specific justification for any “processing,” which would include collection. See GDPR, supra note 266, at 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. at recital 43 (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 Prot. 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[https://perma.cc/MH2G-JGKF] [hereinafter WP Work Opinion].

269. Jacob M. Victor, Comment, The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy, 123 YALE L.J. 513, 516 (2013) (“[T]he 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.”).
that employees need when they have an interest in providing data to the firm but also an interest in its use thereafter.

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.270 These sales should require employee consent, and employers should be prohibited from punishing workers who refuse to consent. These protections would permit workers to opt out of the sharing or demand a price for their consent.

Third, we should regulate employer collection or use of data that transgresses societal norms of dignity and decency.271 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 providing more clarity as to scope would be a welcome development.272 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 property rights in their data, and that the law should recast itself accordingly.

B. Employers as Information Fiduciaries

Another pathway 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: the assignment of fiduciary responsibility. Fiduciaries find themselves in a position of power with respect to another party. Courts and commentators have characterized the exercise of control by the fiduciary in different but related ways: the ability of the fiduciary to exercise discretion in carrying out its tasks;273 the vulnerability of the beneficiary to the fiduciary’s exercise of power and potential

270. Adler-Bell & Miller, supra note 16.
271. 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).
272. Ajunwa, Crawford & Schultz, supra note 20, at 773–75.
273. Zastrow v. J. 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)” (emphasis omitted)); 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.”); see also D. Gordon Smith & Jordan C. Lee, Fiduciary Discretion, 75 OHIO ST. L.J. 609, 610 n.6 (2014) (“The most commonly cited scholarly works in the canon of fiduciary law emphasize the importance of discretion in fiduciary relationships.”).
opportunism;\textsuperscript{274} the trust and confidence reposed in the fiduciary by the beneficiary;\textsuperscript{275} and the reasonable expectations of the parties.\textsuperscript{276} Because of this power, the law places heightened obligations upon fiduciaries to care for those resources and not to betray the trust of the owner.\textsuperscript{277} Within the employment relationship, employers exercise just this type of power vis-à-vis employees in a variety of ways.\textsuperscript{278} But the fiduciary 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.\textsuperscript{279} Like other fiduciaries, the information fiduciary has special responsibilities to individuals for whom the fiduciary holds or controls something of special value: namely, information.\textsuperscript{280} 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.\textsuperscript{281} Because these relationships involve the collection, analysis, use, and

\begin{itemize}
  \item \textsuperscript{274} 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.").
  \item \textsuperscript{275} Wiener v. Lazard Freres & Co., 672 N.Y.S.2d 8, 14 (App. Div. 1998) (inquiring as to whether one party “reposed confidence in another and reasonably relied on the other’s superior expertise and knowledge”).
  \item \textsuperscript{276} Deborah A. DeMott, \textit{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”).
  \item \textsuperscript{277} Jack M. Balkin, \textit{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.”).
  \item \textsuperscript{280} Balkin, \textit{supra} note 277, 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.”).
  \item \textsuperscript{281} Id.
disclosure of sensitive information, the law prohibits information fiduciaries from using 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.”

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 firm; and sometimes it is used by the firm in its relationships with suppliers, customers, and even the broader public. 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 as related to their data.

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. 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. 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. Given the resulting incompleteness, fiduciary duties are justified to balance out the expectations of the parties and prevent opportunism. Moreover, individual employees lack the legal understanding and bargaining strength to negotiate for the appropriate level of protections. 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.

282. Id. at 1208. 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.

283. Smith, supra note 273, at 1402.

284. E.g., Volokh, supra note 262, at 1057; 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.”).

285. See RESTATEMENT (THIRD) OF AGENCY § 1.01 cmt. g (AM. L. INST. 2006) (“As agents, all employees owe duties of loyalty to their employers.”).

286. 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.”).


288. The GDPR understands this power imbalance and will largely not see employee consent as sufficient to justify the processing of workplace data. See GDPR, supra note 266, at art. 7; WP Work Opinion, supra note 268, at 6–7.
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.” The exact nature of the duties imposed upon employers as information fiduciaries would be open to further development. The critical notion would be one of protection: employers would be prohibited from using employee data to harm them opportunistically. The relationship is a complicated one, and we should acknowledge that employees are “information fiduciaries” for the employer as well. Fortunately for employers, a plethora of intellectual property protections, especially trade secret law, steps in to protect them against unfair employee opportunism. 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 Information Governance

A third avenue for better managing employee data would be to bring 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 collects and uses their data. Business organizational law has been remarkably successful in separating employment from ownership. 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 usually only the equity investors. The end result is that all

289. Balkin, supra note 277, at 1205 (emphasis omitted).
290. See Smith & Lee, supra note 273, at 635 (arguing that fiduciary duty should “distinguish the appropriate pursuit of self-interest from the inappropriate pursuit of self-interest” (emphasis in original)).
291. See RESTATEMENT (THIRD) OF AGENCY § 8.01 (AM. L. 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 277, 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 279, at 6 (offering a theory “based on the risks of opportunism that arise when people trust others with their personal information and online experiences”).
293. See supra Part II.B.
295. See 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.”).
other stakeholders, including employees, are fenced out from participation in governance.\textsuperscript{296}

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.\textsuperscript{297} Labor organizations negotiate 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.\textsuperscript{298} Professional athletes in the four major U.S. sports leagues are all unionized and, as discussed earlier, have complex systems of information management as part of their collective bargaining agreements.\textsuperscript{299} But only about one in ten employees is represented by a labor organization, and only 6.3 percent of private sector employees are unionized.\textsuperscript{300}

No doubt the many roadblocks to collective bargaining should be lifted.\textsuperscript{301} But there are other 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, provides for employee selection of representatives within companies’ governance structure.\textsuperscript{302} Codetermination facilitates employee voice at the highest levels of power and would allow employees to push the governing board for better data policies.\textsuperscript{303} Recently two bills in Congress

\begin{flushleft}
\textsuperscript{297} 29 U.S.C. §§ 158(a)(5), (d) (providing for the duty to bargain in good faith). Although data collection and use would generally fall into the terms and conditions category, it is possible that the Board or courts would consider certain kinds of data use to be part of 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).
\textsuperscript{299} See supra Part III.C.
\textsuperscript{300} See supra Part III.C.
\textsuperscript{301} See, e.g., Protecting the Right to Organize (“PRO”) Act of 2019, H.R. 2474, 116th Cong. §§ 104–105 (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).
\textsuperscript{303} For a discussion of an American approach to employee governance participation, including codetermination, see GRANT M. HAYDEN & MATTHEW T. BODIE, RECONSTRUCTING THE CORPORATION: FROM SHAREHOLDER PRIMACY TO SHARED GOVERNANCE 172–83 (2021).
\end{flushleft}
have proposed American versions of codetermination, making it less fanciful an idea than in the past.\footnote{304}

But codetermination is by no means the only model for participatory governance. 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.\footnote{305} Others have suggested management-labor coordination models, such as a hiring hall.\footnote{306} There are also internal governance mechanisms that facilitate employee involvement. With labels such as “self-managed,” “self-actualizing,” and “evolutionary,”\footnote{307} new models of participatory management work within the organizational structure to give workers power over their workplace.\footnote{308} Although these systems generally lie outside formal legal structures, the law could incentivize their adoption and remove existing barriers to their efficacy.\footnote{309} Another option would be works councils—firm-level or worksite-level organizations that consult with management on issues of day-to-day employment.\footnote{310} These councils have had significant success in dealing with workplace issues in Europe.\footnote{311}

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.

\footnote{304. 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 forty percent 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).}

\footnote{305. See Veena Dubal & Sushil Jacob, Escaping the Wage-Slave/Micro-Entrepreneur Binary: Platforms for Liberating Labor, 26 J. AFFORDABLE HOUS. & CMTY. DEV. L. 67, 67 (2017) (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).}

\footnote{306. 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” (emphasis omitted)).}


\footnote{308. 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).}

\footnote{309. 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).}


\footnote{311. Id. at 609–10.}
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.\(^{312}\) Creation of a data council and deference to its determinations could act as a safe harbor against employee claims of privacy intrusion and data confiscation.\(^{313}\)

Each of these proposals has its own strengths and weaknesses, its own scope and parameters. The critical 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, ensure that they receive the benefits of that data, and carve out spaces for entrepreneurial opportunities and autonomy.

**CONCLUSION**

The law relating to the collection and use of employee data needs a reconceptualization. The existing patchwork of privacy laws provides at best uncertain relief, and intellectual property laws largely hand data ownership over to the firm. The law has encased employer power over employee data through limited privacy protections and expanding intellectual property allotments.\(^{314}\) 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.

---

\(^{312}\) Violations of the policy could be considered breach of contract or a deceptive practice akin to those regulated by the Federal Trade Commission under Section 5 of the FTC Act (codified at 15 U.S.C. § 45).

\(^{313}\) 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).

\(^{314}\) See Kapczynski, *supra* note 257, at 1508–14 (discussing how law encases the power of informational capitalists).