Santa Clara University School of Law

Santa Clara Law Review

Volume 63 | Number 1 Article 2

2023

EMPLOYERS AS INFORMATION FIDUCIARIES

Bodie, Matthew T.

EMPLOYERS AS INFORMATION FIDUCIARIES

Matthew T. Bodie*

In order to better protect users from the predations of large tech companies amassing their data, commentators have argued that these companies should be considered information fiduciaries for the purposes of collection, use, storage, and disclosure of that data. This Essay considers the application of the "information fiduciary" label to employers in the context of employee data. Because employers are handling ever greater quantities of employee data, and because that data is becoming more sensitive and potentially damaging to workers if misused, the law should account for this expanded role with expanded protections. The beginnings of how such a set of protections might look is briefly explored.

TABLE OF CONTENTS

* Callis Family Professor and Co-Director, Wefel Center for Employment Law, Saint Louis University School of Law. This article was presented as part of the symposium *What to Expect in the Post-Pandemic New Normal: The Legal and Policy Issues of Returning to Work and Educating Learners in the "New Normal."* Many thanks to my co-panelists Orly Lobel and Brielle Valle, and to our moderator Donald Polden, for a great panel at the Symposium. I also appreciate feedback from participants at the 2022 Fiduciary Law Workshop, including Karen Boxx, Ignacio Cofone, Andrew Gold, Arthur Laby, Ethan Leib, Brett McDonnell, and Dana Brakman Reiser. My thanks to the staff of the *Santa Clara Law Review* for their excellent editing.

I. INTRODUCTION

We generate our data, but our data can also generate us. To some extent, data is simply information about one interaction, or decision, or idea—one small glimpse into something we do or say or choose that, frankly, can seem quite trivial. But data represents who we are, what we think, what we like, what we share, and how we feel. The more data that someone has about you, the more they can know you, understand you, and even manipulate and control you.

Big Data has made ordinary information into valuable material. But value primarily comes at scale. Through a collection of devices and programming, data is now constantly collected throughout our daily lives and used to provide new products, better services, and tailored advertising—what is often called—"surveillance capitalism."[1] The true benefits from this new form of information compilation and analysis come when massive amounts of data are digested using algorithms that find meaningful insights from that data. That is why institutional Big Data players have reached gargantuan scale: their size correlates to their effectiveness. This has also made it harder for ordinary people to assert themselves against these players. If ordinary people want to participate in the information economy—or even just the standard economy, increasingly—they need to hand over their data to those with the data machinery to use it.

When we think of the legal, economic, and social challenges of Big Data, we often focus on the impact of algorithms and machine learning on our roles as consumers and on the conduct of our private lives. But Big Data is transforming the workplace too.[2] Traditionally, workers maintained a separation between their work lives and their personal lives in a sort of rough informational bargain. The divide between personal and employment-related information was meant to protect workers' personal and civic autonomy.

---

1. Shoshana Zuboff, THE AGE OF SURVEILLANCE CAPITALISM (2019).

2. 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—its collection, aggregation, and use—is changing the balance of power in the workplace.").

But this division is breaking down. Personal information related to health, politics, religion, interpersonal skills, and attitudes towards authority can now be ascertained much more easily. And—despite what we might hope—employers can use these wide varieties of information for business ends.[3]

The potential for information exploitation is vast and largely underexplored at this point in time. Information that might seem personal and private can help employers choose whom to hire and fire, select the appropriate composition of workplace teams, and monitor when employees might be most productive.[4] The SARS-CoV-2 pandemic has only exacerbated this blending of the two worlds. At various points throughout the pandemic, employers have taken employees' temperatures, asked their vaccination status, imposed vaccination requirements, and tracked employees' interactions with other employees, customers, and clients.[5] For those working from home, the employer has literally come into the personal sanctum, whether through a work computer, software, webcams, or other methods of monitoring and managing performance.[6]

---

3. *See generally* Matthew T. Bodie, Miriam A. Cherry, Marcia L. McCormick & Jintong Tang, *The Law and Policy of People Analytics*, 88 U. COLO. L. REV. 961, 968-73 (2017) (describing how companies use people analytics to improve workers productivity).

4. Google, for example, uses a data-driven approach to employment conditions 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. LASZLO BOCK, WORK RULES!: INSIGHTS FROM GOOGLE THAT WILL TRANSFORM HOW YOU LIVE AND LEAD 241-42, 261-62, 315 (2015). 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. Charles Duhigg, *What Google Learned from its Quest to Build the Perfect Team*, N.Y. TIMES MAG. (Feb. 25, 2016), https://www.nytimes.com/2016/02/28/magazine/what-google-learned-from-its-quest-to-build-the-perfect-team.html [https://perma.cc/9BX9-HYTA] (finding that teams thrived most when they engendered a sense of psychological safety).

5. Matthew T. Bodie & Michael McMahon, *Employee Testing, Tracing, and Disclosure as a Response to the Coronavirus Pandemic*, 64 WASH U. J.L & POL'Y 31, 34-40 (2021).

6. *See, e.g.*, *id.*; *see also* Mohana Ravindranath, *Coronavirus Opens Door to Company Surveillance of Workers*, POLITICO (June 26, 2020, 4:30 AM), https://www.politico.com/news/2020/06/26/workplace-apps-tracking-coronavirus-could-test-privacy-boundaries-340525 [https://perma.cc/9NFU-9Y4M]; see also Eli Rosenberg, *White House Vaccine Rule Requires Companies and Workers to*

In response to the collapse of personal privacy at work, some commentators have noted the absence of legal support for workers and have proposed additional workplace privacy protections, generally through legislation.[7] In an earlier article, I examined a variety of legal mechanisms that could protect, secure, and empower workers in their relationship with their data.[8] One of those proposals is based on an idea that has gained significant currency in the last few years—that of the "information fiduciary." In its recent guise, the idea is generally attributed to Jack Balkin, but he builds on the work of others who have similarly suggested fiduciary obligations in cyberspace.[9] As developed by Balkin, the concept of information fiduciary puts greater responsibility on companies with high-volume data usage for managing the data in the interests of the data originators.[10] The concept has been met with both approval and skepticism in the context of digital data-traffickers such as Facebook, Google, and Microsoft.[11]

Comply by Jan. 4, WASH. POST (Nov. 4, 2021, 3:28 PM), https://www.washingtonpost.com/business/2021/11/04/white-house-vaccine-mandate/ [https://perma.cc/V4NU-677Y].

7. *See, e.g.*, Ifeoma Ajunwa, Kate Crawford & Jason Schultz, *Limitless Worker Surveillance*, 105 CAL. L. REV. 735, 772-76 (2017) (describing potential reforms in employee privacy protections); Jodi Kantor and Arya Sundaram, *The Rise of the Worker Productivity Score*, N.Y. TIMES, Aug. 14, 2022, https://www.nytimes.com/interactive/2022/08/14/business/worker-productivity-tracking.html ("For frustrated employees, or for companies navigating what to disclose to workers or how to deploy metrics in pay or firing decisions, the law provides little guidance.").

8. *See generally* Matthew T. Bodie, *The Law of Employee Data: Privacy, Property, Governance*, 97 IND. L.J. 707 (2022).

9. *See, e.g.*, DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 102-04 (2004); Ian R. Kerr, *The Legal Relationship Between Online Service Providers and Users*, 35 CAN. BUS. L.J. 419, 446-48 (2001).

10. *See* Jack M. Balkin, *Information Fiduciaries in the Digital Age*, BALKINIZATION (Mar. 5, 2014, 4:50 PM), https://balkin.blogspot.com/2014/03/information-fiduciaries-in-digital-age.html [https://perma.cc/J8DA-ELG4] (developing the idea of an "information fiduciary" and discussing how the concept is reflected in existing fiduciary law).

11. *Compare* Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497, 541 (2019) ("[W]e doubt that the information-fiduciary idea should play any significant role in the struggle to rein in the leading online platforms and reclaim the online public sphere."), *with* Andrew F. Tuch, *A General Defense of Information Fiduciaries*, 98 WASH. U.L. REV. 1897, 1902 (2021) ("Khan and Pozen argue eloquently and emphatically, but their central criticisms significantly overstate the threat that corporate and fiduciary law poses for the information fiduciary model.").

But the idea also works very well—perhaps even better—as applied to employers and their management of employee-related data.

This Symposium contribution makes the case for employers as information fiduciaries. Part II discusses the concept of information fiduciaries and explains some of the controversy about applying this label to large online service providers. Part III explores why the concept would work well as applied to employers with respect to their collection, use, and disclosure of employee data.

II. INFORMATION FIDUCIARIES

The conceit behind the information fiduciary is to take an existing legal tool and refashion it for modern problems. The existing legal tool, in this case, is the concept of a fiduciary. The law asks fiduciaries to take on certain responsibilities to care for another. Those responsibilities are called fiduciary duties, and over time courts have imposed fiduciary duties in a variety of different contexts.[12] Proponents of applying the "information fiduciary" label to large-scale data collectors and users argue that companies handling large sets of personal data should be considered the fiduciaries of those whose data they gather.[13] The structural imbalance of power between Big Tech and its users means that the law should provide a counterbalance in the form of fiduciary duties owed to the users.[14]

To understand Balkin's proposal, it is perhaps useful to explore the concept of the fiduciary. Recent years have seen a significant reinvigoration of fiduciary law and theory, with a greater effort to explain the reasoning behind this legal label for certain kinds of relationships. Traditionally, jurists followed a status-based approach in which the relationship was considered fiduciary in nature if it was categorized as such in the past.[15] There is a competing approach, however, that

12. *See* Deborah A. DeMott, *Beyond Metaphor: An Analysis of Fiduciary Obligation*, 1988 DUKE L.J. 879 (1988) (noting "wide range of situations in which the [fiduciary] obligation may arise.").

13. *See generally* Jack M. Balkin, *The Fiduciary Model of Privacy*, 134 HARV. L. REV. F. 11 (2020).

14. *Id.* at 13-14.

15. Deborah A. DeMott, *Relationships of Trust and Confidence in the Workplace*, 100 CORNELL L. REV. 1255, 1261 (2015) ("Most fiduciary relationships are treated as such as a matter of status or convention.") (quotations omitted);

examines each particular relationship to determine if it potentially fits within the fiduciary framework.[16] Courts and commentators have considered the following to be indicia of fiduciary status: the ability of the fiduciary to exercise discretion in carrying out its tasks;[17] the vulnerability of the beneficiary to the fiduciary's exercise of power and potential opportunism;[18] and the trust and confidence the beneficiary reposes in the fiduciary.[19]

Looking at these characteristics separately, we can get a better sense of the overall picture. For many theorists, the fiduciary's ability to exercise discretion within the relationship is critical. Paul Miller has defined the fiduciary relationship as "one in which one party (the fiduciary) enjoys discretionary power over the significant practical interests of another (the beneficiary)."[20] Gordon Smith has stated that: "fiduciary 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."[21] And Larry Ribstein has argued that fiduciary duties should apply "where an 'owner' who controls and derives

---

Paul B. Miller, *A Theory of Fiduciary Liability*, 56 MCGILL L.J. 235, 241-43 (2011) (stating that courts determine "whether the category is conventionally recognized as fiduciary.").

16. Miller, *supra* note 15, at 243-47.

17. 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.").

18. 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.").

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

20. Miller, *supra* note 15, at 262 (italics omitted); *see also* Paul B. Miller, *The Fiduciary Relationship*, *in* PHILOSOPHICAL FOUNDATIONS OF FIDUCIARY L. 63, 65 (Andrew S. Gold & Paul B. Miller eds., 2014).

21. D. Gordon Smith, *The Critical Resource Theory of Fiduciary Duty*, 55 VAND. L. REV. 1399, 1402 (2002). *See also* D. Gordon Smith & Jordan C. Lee, *Fiduciary Discretion*, 75 OHIO STATE 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.").

the residual benefit from property delegates open-ended management power over property to a 'manager.' "[22] The notion of discretion as critical to fiduciary relationships forms the cornerstone of many fiduciary theories.

Others designate vulnerability as a critical feature of fiduciary relationships. Fiduciary duties function as the beneficiary's protection against vulnerability arising from the power and discretion the fiduciary may exercise.[23] If the beneficiary were able to protect itself—for example, through economic self-help or through contract—fiduciary duties would be superfluous. The open-ended nature of fiduciary relationships, combined with a power imbalance, may subject the beneficiary to the fiduciary's opportunism.[24] Vulnerability is often characterized as dependency: the beneficiary is dependent on the fiduciary's discretion or good graces within the relationship.[25] This link between power/discretion and vulnerability/dependency is a critical justification for the fiduciary relationship.[26]

The need for trust and confidence is interrelated with concerns about discretion and vulnerability. In these types of relationships, the fiduciary must exercise discretion in a way that is hard for the beneficiary to police contractually and

---

22. Larry E. Ribstein, *Are Partners Fiduciaries?*, 2005 U. ILL. L. REV. 209, 215 (2005); *see also* Larry E. Ribstein, *Fencing Fiduciary Duties*, 91 B.U. L. REV. 899, 901 (2011) ("[M]y definition [of fiduciary relationships] focuses on the particular type of entrustment that arises from a property owner's delegation to a manager of open-ended management power over property without corresponding economic rights.").

23. *See, e.g.*, Lawrence E. Mitchell, *Trust. Contract. Process.*, *in* PROGRESSIVE CORP. L. 185, 190 (Lawrence E. Mitchell ed., 1995) ("Fiduciary relationships are, characteristically, relationships of power and dependency.").

24. Smith & Lee, *supra* note 21, at 620 ("Although incomplete contracts are inevitable, contracting parties routinely create fiduciary relationships, in which one party (the beneficiary) seems especially vulnerable to opportunism by the counterparty (the fiduciary).").

25. Miller, *supra* note 15, at 254 ("Dependence is usually taken to mean that certain interests of the beneficiary are subject to influence by the fiduciary.").

26. Smith & Lee, *supra* note 21, at 620 n.54; Evan J. Criddle, *Fiduciary Administration: Rethinking Popular Representation in Agency Rulemaking*, 88 TEX. L. REV. 441, 470 (2010) ("[A]ll beneficiaries are vulnerable to the fiduciary's abuse of legally entrusted administrative power over their legal and practical interests."); Evan Fox-Decent, *The Fiduciary Nature of State Legal Authority*, 31 QUEENS L.J. 259, 275 (2005) (asserting that a fiduciary obligation arises "whenever one party unilaterally assumes discretionary power of an administrative nature over the important interests of another, interests that are especially vulnerable to the fiduciary's discretion.").

privately, rendering beneficiaries vulnerable.[27] But the beneficiary has no choice except to trust that the fiduciary will act in their best interests; that is the nature of the relationship. As Balkin describes it, the fiduciary relationship should cover situations in which "the stronger party has issued an implicit or explicit invitation to trust that the weaker party has accepted."[28]

When the law imposes fiduciary duties upon a relationship, it assigns a set of responsibilities owed by the fiduciary to the beneficiary. Those duties vary in kind, scope, and degree, depending on the nature of the relationship.[29] The two central fiduciary duties are the duty of care and the duty of loyalty.[30] The duty of care requires the fiduciary to exercise a certain level of attention and prudence in handling their responsibilities, often characterized as "due" care or a reasonable level of care.[31] The duty of loyalty requires the fiduciary to act in the interests of the beneficiary—to put aside its own self-interest and act with the beneficiary's interests in mind.[32] Together, the duty of care and the duty of loyalty require the fiduciary to act with a certain level of attentiveness

---

27. Evan J. Criddle, *Fiduciary Administration: Rethinking Popular Representation in Agency Rulemaking*, 88 TEX. L. REV. 441, 470 (2010); DeMott, *supra* note 12, at 902 ("In many relationships in which one party is bound by a fiduciary obligation, the other party's vulnerability to the fiduciary's abuse of power or influence conventionally justifies the imposition of fiduciary obligation.").

28. Balkin, *supra* note 13, at 13.

29. Khan & Pozen, *supra* note 11, at 510 (noting that "fiduciary duties are not one-size-fits-all in the law, and . . . they can and do vary from context to context.").

30. Rob Atkinson, *Obedience as the Foundation of Fiduciary Duty*, 34 J. CORP. L. 43, 45 (2008) ("Commentators, both doctrinal and theoretical, have come to agree that the fiduciary relationship rests on twin pillars, the duty of care and the duty of loyalty."); Jack M. Balkin, *Information Fiduciaries and the First Amendment,* 49 U.C. DAVIS L. REV. 1183, 1207-08 (2016).

31. *See* John C.P. Goldberg, *The Fiduciary Duty of Care*, *in* THE OXFORD HANDBOOK OF FIDUCIARY L. 405, 406 (Evan J. Criddle, Paul B. Miller & Robert H. Sitkoff eds., 2019) (describing the duty of care as "exercising the prudence that an ordinarily prudent person would have exercised under the circumstances.").

32. Andrew Gold, *The Fiduciary Duty of Loyalty*, *in* THE OXFORD HANDBOOK OF FIDUCIARY L., 385, 386 (Evan J. Criddle, Paul B. Miller & Robert H. Sitkoff eds., 2019); Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U.L. REV. 961, 987 (2021) ("The core idea animating a duty of loyalty is that trusted parties must make their own interests subservient to those made vulnerable through the extension of trust.").

and thoughtfulness, forswearing opportunities to take advantage of the other party through the relationship.

Along with these two primary duties, other fiduciary duties have at times been applied as a part of fiduciary responsibilities. The duty of obedience is often cited as an important aspect of the relationship, and it is characterized as either a duty to obey the instructions of the fiduciary, or a duty to obey the law.[33] The duty of confidentiality is also seen as critical to certain fiduciary relationships.[34] Other duties include the duty to act only within the scope of the agent's authority,[35] the duty to act reasonably within the scope of the agency relationship,[36] and the duty to provide information to the principal/beneficiary.[37]

Information management is always important within a fiduciary relationship. Some fiduciary duties, such as the duty of confidentiality or the duty to provide information, focus on the exchange of information between the parties. But all fiduciary duties depend to some extent on communication and the need for the beneficiary to have a proper understanding of underlying context in order to direct and assess their fiduciary within the relationship.[38] Even within the category of fiduciary relationships, there is a subcategory of "information fiduciaries" that turns explicitly on the role of information and its importance.[39]

The idea of the information fiduciary is less a doctrinal category than a descriptive one. The most recent set of

---

33. *Compare* Atkinson, *supra* note 30, at 45-46 (describing "the agent's duty to obey the will of the principal" as fundamental to the fiduciary relationship), *with* Alan R. Palmiter, *Duty of Obedience: The Forgotten Duty,* 55 N.Y.L. SCH. L. REV. 457, 458 (2010-2011) (stating that the duty of obedience "compel[s]corporate fiduciaries to abide by legal norms—both those of the corporation and of external law.").

34. *See, e.g.*, RESTATEMENT (THIRD) OF AGENCY § 8.05 (2006) ("An agent has a duty . . . (2) not to use or communicate confidential information of the principal for the agent's own purposes or those of a third party.").

35. *Id.* § 8.09 ("An agent has a duty to take action only within the scope of the agent's actual authority.").

36. *Id.* § 8.10.

37. *Id.* § 8.11 ("An agent has a duty to use reasonable effort to provide the principal with facts that the agent knows, has reason to know, or should know . . ..").

38. *Cf.* Balkin, *supra* note 30, at 1208 ("Relationships of trust and confidence are often centrally concerned with the collection, analysis, use, and disclosure of information.").

39. *Id.* at 1186-87.

discussions around the term stems from a proposal by Jack Balkin.[40] According to Balkin: "[a]n 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."[41] Many professionals who keep their clients' information confidential, such as doctors and lawyers, are essentially information fiduciaries.[42] Because these relationships involve the collection, analysis, use, and 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."[43] Like other fiduciaries, the information fiduciary has special responsibilities to individuals for whom the fiduciary holds or controls something of special value, but in this case, the fiduciary's control is largely limited to information itself.[44]

In elucidating the concept of an information fiduciary, Balkin was endeavoring to reconceive the legal relationship between large digital information hubs and their users—essentially, "all businesses that collect information from end users in return for their services."[45] Because these businesses collect, use, and disclose such information during business operations, users must trust them to use this information appropriately.[46] This trust renders users "increasingly dependent on and vulnerable to" these businesses and their data management decisions.[47] By characterizing Big Tech companies like Google, Facebook, and Microsoft (and many others) as information fiduciaries, these large online service

40. *See* Balkin, *supra* note 10 (developing the idea of an "information fiduciary" and discussing how the concept is reflected in existing fiduciary law); *see also* Khan & Pozen, *supra* note 11, at 499 (discussing how Kenneth Laudon appears to have coined the term in 1990).

41. Balkin, *supra* note 30, at 1209.

42. *Id.*

43. *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.

44. Balkin, *supra* note 30, at 1209.

45. Balkin, *supra* note 13, at 17.

46. *Id.* at 11.

47. *Id.* at 11.

providers would be legally restrained in their collection, use, and disclosure of user data.[48]

Like many other observers,[49] Balkin believes that current law fails to properly protect users in their data relationships with online service providers.[50] U.S. law is primarily oriented around a system of notice and consent, whereby users are notified of data collection (and sometimes use and disclosure) and asked to give their consent to whatever practices are in place.[51] The model imagines an educated and perspicacious user who is aware of and thoughtful about the particular company's data practices and assesses whether it makes sense to participate in the exchange. The problems with a notice-and-consent regime, however, are evident when considering the amount of time it would take to read each proposed contract regarding data, let alone to be educated about the actual practices proposed.[52] As Balkin points out, the contractual terms rarely bind the online service providers in a meaningful way.[53] Instead, contractual terms frequently allow companies to control the terms of engagement, change conditions over time, and keep aspects of data use hidden.[54] There are also meaningful third-party effects on parties outside of the contractual relationship.[55] Ultimately, a contract alone is insufficient to protect users from opportunistic use of their data in ways that are counter to their interests, with no real opportunity for them to object other than cutting themselves off from the service.

If online data collectors are labeled as information fiduciaries, the relationship would change from contract-only to contract-plus. Fiduciary obligations are meant to protect the vulnerable and rebalance the scale between the parties. Balkin references other information fiduciaries such as doctors

48. Balkin, *supra* note 10.

49. *See, e.g.*, Richards & Hartzog, *supra* note 32, at 967.

50. Balkin, *supra* note 13, at 16-18.

51. Anupam Chander, Margot E. Kaminski & William McGeveran, *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733, 1747-48 (2021).

52. There are numerous entries in this genre. *See, e.g.*, Geoffrey A. Fowler, *I tried to read all my app privacy policies. It was 1 million words.*, WASH. POST (May 31, 2022, 7:00 AM), https://www.washingtonpost.com/technology/2022/05/31/abolish-privacy-policies/.

53. Balkin, *supra* note 13, at 16-17.

54. *Id.* at 16.

55. *Id.* at 17.

and lawyers and points to their duties of care, loyalty, and confidentiality.[56] He acknowledges that our expectations of confidentiality may be different for professional advisors, whose relationships may be much more intimate and meaningful, and their information about us potentially much more damaging.[57] However, online service providers may have a broader spectrum of data and much higher volume across the board. Balkin wants fiduciary duties in place to protect against unfair efforts to take advantage of the data in unfair ways, such as threatening to embarrass critics, surreptitiously trying to influence elections, or otherwise "us[ing] the data in unexpected ways to the disadvantage of people who use their services or in ways that violate some other important social norm."[58] As an example, Balkin points to Facebook and its decision to allow third parties to access and exploit private user data without their knowledge, as illustrated by the Cambridge Analytica scandal.[59]

If this sounds somewhat vague, it is intentionally and perhaps necessarily so.[60] Fiduciary duties are not regulatory prescriptions; they are not specific mandates. They are instead efforts to fill in the gaps in a more rigorous way than the standard duty of good faith would allow in a contract.[61] Where Balkin leaves most of the details for further development, Neil Richards and Woodrow Hartzog have developed a more rigorous framework regarding the duty of loyalty as applied to online data collectors.[62] Richards and Hartzog would apply their duty of loyalty in circumstances similar to, but broader than, Balkin: "[l]oyalty should be required (1) when trust is

56. *Id.* at 14-15.

57. *Id.* at 15; Balkin, *supra* note 30, at 1225-26.

58. Balkin, *supra* note 30, at 1227.

59. Jack M. Balkin, *Free Speech is a Triangle*, 118 COLUM. L. REV. 2011, 2049-53 (2018).

60. Balkin, *supra* note 30, at 1229 ("What is unexpected or seems like a breach of trust will depend on the kind of service that entities provide and what we would reasonably consider unexpected or abusive for them to do. Because there are so many possible online services, including services nobody has yet imagined, legislatures and courts may find it difficult to draw lines initially."); *see also* Robert H. Sitkoff, *Other Fiduciary Duties: Implementing Loyalty and Care*, *in* THE OXFORD HANDBOOK OF FIDUCIARY L., 419, 419 (Evan J. Criddle, Paul B. Miller & Robert H. Sitkoff eds., 2019).

61. *But cf.* Khan & Pozen, *supra* note 11, at 523 (accusing Balkin of merely wanting to impose a duty of good faith on online service providers).

62. Richards & Hartzog, *supra* note 32, at 1003-12.

invited, (2) from people made vulnerable by exposure, (3) when the trustee has control over people's online experiences and data processing, and (4) when people trust data collectors with their exposure."[63] Their description of loyalty also has its gray areas, but it specifically highlights these types of obligations: not collecting or using data against the interests of users; requiring data minimization and purpose limitations on use; imposing a "duty of honesty" based on a genuine effort to inform; and disallowing any purported waivers of the duty.[64] Ultimately, Richards and Hartzog would institute this "simple maxim: When in doubt, be loyal to those who trusted you with their exposure."[65]

Despite the known unknowns in the contours of a fiduciary relationship, supporters of the information fiduciary approach believe it will have a salutary effect on relations between Big Tech data companies and their users. Balkin is quick to point out that he thinks the fiduciary label is best understood as a complement to, and not a replacement for, other types of regulation.[66] He does worry that the First Amendment will offer special challenges to regulation of online platforms such as Facebook and Google, and that the fiduciary label might blunt the power of constitutional objections.[67] He also may favor a lighter regulatory touch, as he seems comfortable with practices such as data-targeted advertising that others would reject.[68] But Balkin is clear that the application of the information fiduciary label would be just one aspect of the overall legal framework.

Not everyone is on board with Balkin's approach. Lina Khan and David Pozen believe that the tool is not equipped for the task, as companies like Facebook and Google present very different challenges for the general public than do doctors and

63. *Id.* at 1004.

64. *Id.* at 997-1003.

65. *Id.* at 1003.

66. *See* Balkin, *supra* note 13, at 20-21.

67. Balkin, *supra* note 30, at 1209 ("The First Amendment treats information practices by fiduciaries very differently than it treats information practices involving relative strangers.").

68. *Compare* Balkin, *supra* note 13, at 27-28 (questioning whether "all targeted advertising is inherently abusive and inconsistent with the best interests of end users"), *with* Richards & Hartzog, *supra* note 32, at 1019 ("Under our approach, targeted ads could not continue in their current form but might continue if they are pursued in a transparent and loyal manner.").

lawyers.[69] They worry that support for Balkin's proposal will "cannibalize" support for more meaningful structural reform such as antitrust actions, common carrier regimes, interoperability requirements, and public options.[70] They also raise concerns about applying competing sets of fiduciary duties on corporations, whose directors already have duties of loyalty to shareholders and to the corporation.[71] However, as Andrew Tuch has convincingly explained, their apprehension comes from a misapprehension about the application of fiduciary duties in these contexts; Balkin's duties would apply to the corporation, not its directors.[72]

Rather than throwing out the concept of fiduciary duties, Claudia Haupt instead argues that we should reconsider its underlying analogy.[73] She points to trustees, rather than doctors, lawyers, and other professionals, as the better way of thinking about information fiduciaries.[74] A trustee assumes "a fiduciary responsibility for managing the trust assets and carrying out the purposes of the trust."[75] Just as trustees must oversee a store of valuables in the best interests of the trust's beneficiaries, information fiduciaries oversee a store of data in the best interests of those who provided the data.[76] Although Haupt acknowledges that this approach may conceive of data as property, she does see useful comparisons between the trustee's property-management function and the platform's information-management function.[77]

When we designate a doctor, an accountant, a trustee, or an online service provider as an "information fiduciary," we

---

69. *See generally* Khan & Pozen, *supra* note 11, at 506-11.

70. *Id.* at 537-38.

71. Khan & Pozen, *supra* note 11, at 508-09.

72. Tuch, *supra* note 11, at 1908-11 (explaining the difference between fiduciary duties on the part of directors as opposed to fiduciary duties on the part of corporations); *id.* at 1911-16 (discussing the broad scope of discretion that directors have within the fiduciary context); *id.* at 1916-21 (citing to the corporation's and directors' overarching duty to follow the law); *id.* at 1925-34 (contending that Khan and Pozen's concerns about the misalignment of interests is overstated).

73. Claudia E. Haupt, *Platforms as Trustees: Information Fiduciaries and the Value of Analogy*, 134 HARV. L. REV. F. 34, 35 (2020) (comparing information fiduciaries to trustees rather than professionals).

74. *Id.* at 35.

75. *Id.* at 37.

76. *Id.* at 37-38.

77. *Id.* at 40.

recognize the significant degree of trust given to others in holding our data in their care. The information economy forces participants to trust their data to others for safekeeping, even when that trust may not come naturally. The legal designation is meant to bolster the necessity of trust with potential ramifications for failure to uphold that trust. As it happens, many employees are forced to trust their employers with important personal data across a variety of metrics. These employers too should be considered information fiduciaries.

III. EMPLOYERS AS INFORMATION FIDUCIARIES

Employers have long collected, processed, analyzed, and disclosed worker data. Surveillance—or observation, using its more anodyne nomenclature—is fundamental to the control that an employer exercises over employees.[78] Developed in the late nineteenth Century, scientific management focused on direct observation of workers, paired with analysis of the data collected from those observations.[79] As the field of personnel management has developed, workers were no longer deemed cogs in a machine but rather individual people, replete with their own personalities and peccadillos.[80] Henry Ford's

78. *See, e.g.*, Ajunwa, Crawford & Schultz, *supra* note 7, 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.").

79. 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* Fred 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).

80. *See* BRUCE E. KAUFMAN, THE ORIGINS & EVOLUTION OF THE FIELD OF INDUSTRIAL RELATIONS IN THE UNITED STATES 24-25 (1993); *see also* GORDON S. WATKINS, AN INTRODUCTION TO THE STUDY OF LABOR PROBLEMS 476-77 (Seba Eldridge ed. 4th ed. 1922) ("The old scientific management failed because it was not founded upon a full appreciation of the importance of the human factor . . . It

Sociological Department famously delved into his workers' personal lives, with 150 investigators on hand to collect information on their personal habits and vices.[81] But the early tools to collect data on employees pale in comparison to what is available now. The collection of quantitative data about employees and the analysis of that data using complex algorithms has sometimes been referred to as "people analytics."[82] Employers can collect data from workers' use of the internet; their email, text messaging, and oral communications; their movements throughout the day, even down to their hand and arm motions; their heart rate, body temperature, and other health data.[83] Methods of interaction that are automatically recorded have made the collection of worker communications relatively costless for employers.[84] Systems of artificial intelligence can then conduct increasingly sophisticated and nonintuitive analyses on this data to evaluate employee performance.[85] Google provides one example. Its "People Operations"[86] department has used data analytics to recommend pay practices with higher differentials,

---

was left to the new science of personnel management to discover and evaluate the human elements in production and distribution.").

81. Samuel M. Levin, *Ford Profit Sharing, 1914-20: 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 investigators "examine[d] home conditions, to find out whether a man drinks, how he spends his evenings, whether he has a bank account, dependents, etc."); M. Todd Henderson, *The Nanny Corporation*, 76 U. CHI. L. REV. 1517, 1541 (2009). Ford later disbanded the Sociological Department and stated: "Welfare work that consists in prying into employees' private concerns is out of date." HENRY FORD, MY LIFE AND WORK 130 (1922).

82. *See generally* Bodie, Cherry, McCormick & Tang, *supra* note 3, at 964-73.

83. *See generally* Ajunwa, Crawford & Schultz, *supra* note 7.

84. *See* Ajunwa, Crawford & Schultz, *supra* note 7, at 738. Recent innovations in worker data collection include a "smart" office chair cushion that records bad posture, heart rates, and time away from the chair. 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].

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

86. Adam Bryant, *Google's Quest to Build a Better Boss*, N.Y. TIMES (Mar. 12, 2011), https://www.nytimes.com/2011/03/13/business/13hire.html [https://perma.cc/P2S5-8T7K] (noting that "'people operations' . . . is Googlespeak for human resources.").

smaller plate sizes in the cafeteria, and use of personality types to compose worker teams.[87]

The COVID-19 pandemic has exacerbated an already expanding trend: the collection of employee data hitherto considered personal.[88] Data-based approaches to human resources management seek out pools of information that offer new perspectives on employee productivity.[89] While much of this data involves workplace activity, employers increasingly understand the connections between personal life and business success.[90] Most obviously, employee personal health, although considered private, undoubtedly affects work performance.[91] When the pandemic hit, "[t]he distinction between work and everything else, already a blurry line for most Americans, got even blurrier."[92] When physically present on the job, co-workers can be a nexus of infection and contagion; your neighbor on the meatpacking line, for example, could give you COVID.[93] Early in the pandemic, some employers used testing,

87. LASZLO BOCK, WORK RULES!: INSIGHTS FROM GOOGLE THAT WILL TRANSFORM HOW YOU LIVE AND LEAD 241-42, 261-62, 315 (2015); Charles Duhigg, *What Google Learned from its Quest to Build the Perfect Team*, N.Y. TIMES MAG. (Feb. 25, 2016), https://www.nytimes.com/2016/02/28/magazine/what-google-learned-from-its-quest-to-build-the-perfect-team.html [https://perma.cc/9BX9-HYTA] (discussing team composition using personality).

88. Ajunwa, Crawford & Schultz, *supra* note 7, at 738-39 ("What is novel, and of real concern to privacy law, is that rapid technological advancements and diminishing costs now mean employee surveillance occurs both inside and outside the workplace—bleeding into the private lives of employees."); Leora F. 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.").

89. Dave Zielinski, *Employers Increased Employee Data Collection During Pandemic*, SHRM (Dec. 1, 2020), https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/employers-increased-employee-data-collection-during-pandemic.aspx.

90. *See, e.g.*, Jasmina Žnidaršič & Mojca Bernik, *Impact of Work-Family Balance Results on Employee Work Engagement Within the Organization: The Case of Slovenia*, PLOS ONE (Jan. 20, 2021), https://doi.org/10.1371/journal.pone.0245078.

91. Jenna Wortham, *The Rise of the Wellness App*, N.Y. TIMES MAG. (Mar. 4, 2021), 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).

92. *Id.*

93. *See* Jill Colvin, *Trump order keeps meatpacking plants open, but unions say workers unsafe,* CHI. TRIB. (Apr. 29, 2020, 11:43 AM),

tracing, and disclosure programs to contain the spread of the disease; these programs collected lots of sensitive employee data.[94] Many workers brought employers (and their data collection efforts) into their homes, compounding trends that had already exposed home and personal life to employer observation, especially through social media posting.[95] We are watching the wholesale disintegration of the personal/business divide.[96]

With these increasing levels of data collection and processing, employers have amassed truly colossal levels of information about their employees—information that is often sensitive, personal, and potentially embarrassing or even humiliating. Workers do have some privacy protections, whether it be personal choices like not having a smartphone, or legal prohibitions against certain kinds of employer invasions.[97] But as I have discussed elsewhere, privacy protections within the workplace are quite weak.[98] Cobbled together from a hodgepodge of various statutory and common-

https://www.chicagotribune.com/coronavirus/ct-nw-coronavirus-trump-slaughterhouse-meatpacking-20200429-34sj5c3neray7jrylc7l3pnnfm-story.html.

94. *See* Bodie & McMahon, *supra* note 5; Dave Zielinski, *Employers Increased Employee Data Collection During Pandemic*, SHRM.ORG, (Dec. 1, 2020), https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/employers-increased-employee-data-collection-during-pandemic.aspx.).

95. Megan Brenan, *COVID-19 and Remote Work: An Update*, GALLUP (Oct. 13, 2020), https://news.gallup.com/poll/321800/covid-remote-work-update.aspx [https://perma.cc/YPR3-9WKU] (showing that roughly 50% of employees worked from home early in the pandemic); *see also* Nicholas Bloom, *How Working from Home Works Out*, STAN. INST. FOR ECON. POL'Y RSCH. (June 2020), https://siepr.stanford.edu/research/publications/how-working-home-works-out [https://perma.cc/KL2R-8T7N] (finding that 42 percent of workers were primarily working at home). Many companies have publicly changed their work-from-home policies indefinitely. *See, e.g.*, Carlie Porterfield, *Facebook Will Allow Nearly All Employees to Work Remotely Post-Pandemic*, FORBES (June 9, 2021, 2:39 PM), https://www.forbes.com/sites/carlieporterfield/2021/06/09/facebook-will-allow-nearly-all-employees-to-work-remotely-post-pandemic/?sh=2629b35326a7 [https://perma.cc/5Q8E-LPVX].

96. Ajunwa, Crawford & Schultz, *supra* note 7, 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.").

97. For an overview of employee privacy protections, see Matthew T. Bodie, *The Law of Employee Data: Privacy, Property, Governance*, 97 IND. L.J. 707, 717-27 (2022).

98. *Id.* at 733 ("The law has endeavored to provide some space for personal privacy and autonomy in the workplace, but those efforts are growing increasingly quixotic.").

law doctrines, the employment privacy regime offers primarily procedural protections, such as the necessity of notice and consent, within a generous presumption of employer discretion.[99] Some of the nation's strongest privacy regimes, such as HIPAA[100] and the California Consumer Privacy Act,[101] explicitly exclude employee data from their coverage. Because most privacy regimes are waivable if consent is given, employers can condition employment on such a waiver, making privacy law countenance even the most shocking of invasions.[102] At the same time, intellectual property regimes have ensured that the employer holds the rights to the continuing use of the data as part of an algorithm, artificial intelligence, or even automated versions of the employees' labors.[103] Trade secret law protects algorithms stocked with worker data; the work-for-hire doctrine in copyright insures that employee creations remain in employer hands; trademark ensures that the employer can prevent former employees from trading on the company's name and reputation.[104] Employers hold the legal rights over the employee data they collect with few restrictions on collection, retention, and use.

This unfair situation needs to be rebalanced, and the concept of the information fiduciary is uniquely positioned to do so. Balkin's definition of 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."[105] Critical to the concept are the themes of trust and vulnerability that arise when one party holds such massive quantities of information about the other.[106] Because information fiduciaries "invite

99. *Id.* at 717-24.

100. 45 C.F.R. § 160.103 (2020) (defining "covered entity" as a health plan, a health care clearinghouse, or a health care provider). Employers are not covered unless they provide health care or self-administered health insurance coverage. *Id.* §§ 164.103, 164.105.

101. The California Consumer Privacy Act only requires that the employer 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).

102. *See, e.g.*, Feminist Women's Health Ctr. v. Superior Ct., 61 Cal. Rptr. 2d 187 (Cal. Ct. App. 1997).

103. Bodie, *supra* note 8, at 724-29.

104. *Id.*

105. Balkin, *supra* note 30, at 1209.

106. Balkin, *supra* note 13, at 11.

people to trust them with their data," the data providers "become vulnerable: to how the companies use their data, to companies' data security (or lack thereof), and to companies' choice to share or sell the data to others."[107] This vulnerability and dependence require a counterweight to protect the individuals whose data is in play. By applying fiduciary duties to the data holders, society can protect the vulnerable from opportunistic exploitation.

To my knowledge, neither Balkin nor the others who have supported (or critiqued) his proposal have envisioned the information fiduciary label as applied to employers. But the label fits. A thick stream of information is constantly flowing from worker to employer. This torrent pours in from many different tributaries and ranges from everyday observation to deeply personal revelations. Legal efforts to put up walls of privacy between employer and employee have largely failed, in part because of acquiescence to forced consent and in part because of the necessity of information exchange.[108] Employees may strongly desire to not share information about their personal health, hidden disabilities, or family schedules, but sharing is often required, and workers may even find such sharing beneficial in certain circumstances.[109] As Big Data techniques grow cheaper, more powerful, and more widespread, the information flow between employer and employee has become a raging river.

As this information exchange has begun to overflow the banks, workers find themselves increasingly vulnerable to employers. Like the online service providers discussed by Balkin, employers may know a lot about us, but we do not know a lot about them.[110] The massive information asymmetries give management significant power over employees without any

---

107. *Id.*

108. Bodie, *supra* note 8, at 724 ("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.").

109. For example, an employee may share information about an illness to request medical leave, share information about a disability to receive an accommodation, or share information about family schedules to change a work obligation. *See, e.g.*, 29 U.S.C.A. § 2612(a)(1) (requiring employers to provide leave under certain circumstances relating to family or medical exigencies); 42 U.S.C.A. § 12112(b)(5) (requiring employers to make reasonable accommodations for disabilities).

110. Balkin, *supra* note 13, at 11.

counterbalance. Like other data collectors, employers also enjoy "the asymmetry in power that occurs because one party controls the design of applications and the other must operate within that design."[111] By definition, under the common law, employees are those who the employer has the right to control when acting within the scope of employment.[112] The employer controls the circumstances under which data is collected, processed, and distributed, often without any input from the data providers themselves. The resulting asymmetry leads to genuine vulnerability, with "potential dangers of abuse, manipulation, self-dealing, and overreaching by the more powerful party."[113]

Because of the overall nature of the employment relationship, the law should designate employers as general fiduciaries of their employees.[114] After all, the concerns about employer discretion and control over employment, and the concomitant worker vulnerability it engenders, apply beyond the realm of employee data. But there are special reasons to apply the information fiduciary label even in the absence of the broader designation. The idea that the employer—generally a business organization such as a corporation or partnership—must look out for the best interests of its employees may seem amorphous and unbound.[115] But when employers become repositories of so much employee information that is personal, powerful, and subject to exploitation, it makes sense to focus in on this facet of the employment relationship and apply this particular set of doctrinal protections. Employer collection and

111. *Id.* at 12.

112. RESTATEMENT (SECOND) OF AGENCY § 2(2) (1958) ("[A]n agent employed by a master to perform service in his affairs whose physical conduct in the performance of the service is controlled or is subject to the right to control by the master."); *see also* RESTATEMENT (THIRD) OF AGENCY § 7.07(3)(a) (2006) (defining an employee as "an agent whose principal controls or has the right to control the manner and means of the agent's performance of work."); R. H. Coase, *The Nature of the Firm*, 4 ECONOMICA 386, 404 (1937) (noting that under the traditional common law, the master must have the "right to control the servant's work," which means "being entitled to tell the servant when to work (within the hours of service) and when not to work, and what work to do and how to do it.").

113. Balkin, *supra* note 13, at 15.

114. Matthew T. Bodie, *Employment as Fiduciary Relationship*, 105 GEO. L.J. 819, 862 (2017) ("The employment relationship is best understood as a mutual set of fiduciary relationships between employer and employee.").

115. *But see id.* at 865.

use of employee data is a unique problem, and it deserves specific efforts to address its inequities.

As is often the case with proposed fiduciary responsibilities, an immediate objection is: why not contractual protections? If workers really wanted to constrain and manage employers' use of their data, they could easily add such terms to the employment contract. There is, of course, voluminous literature as to why employees cannot sufficiently protect themselves through contracts.[116] But Balkin's five reasons as to why contract is insufficient to protect users of online service providers apply similarly to employees: (1) the inability to assess the risk of future harm based on data practices; (2) a lack of appreciation for how the data might be combined and used to draw "surprising and powerful inferences about them[selves];" (3) the control exercised by the data collectors over the environment; (4) the leveraging of emotions and cognitive limitations to shape behavior; and (5) external effects on third parties from the gathering and use of data.[117] Regarding this final point, Balkin repeatedly mentions how third parties may find data about themselves flowing into the data coffers of Big Tech even if they have no direct relationship with such companies.[118] The same goes for the family, friends, and relations of workers, who may find their personal information kept within the employer's data stores as a byproduct of the information exchange.

The duty of loyalty has similar applications in the data context. Richards and Hartzog argue for the imposition of the duty of loyalty "(1) when trust is invited, (2) from people made vulnerable by exposure, (3) when the trustee has control over people's online experiences and data processing, and (4) when people trust data collectors with their exposure."[119] These factors apply with similar force to employers. Employers invite

116. *See, e.g.*, Samuel R. Bagenstos, *Consent, Coercion, and Employment Law*, 55 HARV. C.R.-C.L. L. REV. 409, 465 (2020) (discussing "the value of regulation and collective bargaining in promoting meaningful freedom for workers"); Aditi Bagchi, *The Myth of Equality in the Employment Relation*, 2009 MICH. ST. L. REV. 579, 580 (2009) (noting that "employers and employees are not on equal footing" and that the "inequality between them is multi-dimensional."); Guy Davidov, *The Three Axes of Employment Relationships: A Characterization of Workers in Need of Protection*, 52 U. TORONTO L.J. 357, 361-62 (2002).

117. Balkin, *supra* note 13, at 16-17.

118. *See, e.g.*, *id.* at 17.

119. Richards & Hartzog, *supra* note 32, at 1004.

their employees to provide all manner of sensitive information to them, rendering employees vulnerable by dint of the exchange.[120] Employers design and control the interfaces through which employee information is provided and collected, like online service providers. Employees therefore must place their trust in employers—even if, like online users, that trust is given grudgingly.[121] As Richards and Hartzog advise: "loyalty is specifically tailored to prevent the full range of opportunistic behavior that stems from such a steep power imbalance and deep exposure of ourselves to the whims of those who would otherwise strip us for parts."[122]

As in the application of fiduciary duties to online service providers, the "information fiduciary" label is meant to supplement, not replace, other forms of regulation. Employment relationships are regulated in myriad ways, including fiduciary ones.[123] Under the Employee Retirement Income Security Act (ERISA), [124] administrators of ERISA pension or welfare plans have the same responsibilities as trustees when administering the plan,[125] with four primary fiduciary duties.[126] As already discussed, however, there is little protection for employees when it comes to the employer's use of their information. Employers have no overall duties with regard to the collection, use, or disclosure of employee data. HIPAA does not cover health-related information in the employment context. Employers do not, under current law, even assume a duty to keep sensitive employee data confidential.[127] The *Restatement of Employment Law* adopted

120. One of the potential vulnerabilities for online users mentioned by Richards and Hartzog is the possibility that information will be "used to deny people employment opportunities." *Id.* at 1005.

121. *Id.* at 1007.

122. *Id.* at 1008.

123. Brett H. McDonnell & Matthew T. Bodie, *From Mandates to Governance: Restructuring the Employment Relationship*, 81 MD. L. REV. 887, 889-90 (2022).

124. Employee Retirement Income Security Act of 1974, Pub. L. No. 93-406, 88 Stat. 829 (codified as amended in scattered sections of 26 and 29 U.S.C.).

125. Metro. Life Ins. Co. v. Glenn, 554 U.S. 105, 111 (2008) (stating that courts "should analogize a plan administrator to the trustee of a common-law trust" and "should consider a benefit determination to be a fiduciary act.").

126. These fiduciary duties are: the duty of loyalty to plan participants, 29 U.S.C. § 1104(a)(1)(A) (also known as the exclusive benefit rule); the duty of prudence, *id.* § 1104(a)(1)(B); the duty of prudent diversification of plan assets, *id.* § 1104(a)(1)(C); and the duty to follow plan terms, *id.* § 1104(a)(1)(D).

127. Scott L. Fast, *Breach of Employee Confidentiality: Moving Toward a Common-Law Tort Remedy*, 142 U. PA. L. REV. 431, 432 (1993) ("[T]here is no

a quasi-confidentiality-based theory in finding that employees have a protected privacy interest "in personal information related to the employee that is provided in confidence to the employer."[128] The employer is liable in tort for providing such confidential information to third parties without consent, if such disclosure is highly offensive.[129] However, the duty only applies "if the employer has promised, by words or conduct, to keep the information confidential or if the employer is required by law to maintain confidentiality."[130]

Assigning the role of information fiduciaries to employers would thus address a critical gap in labor and employment law with a flexible yet meaningful framework. Common law already recognizes fiduciary duties within the employment context; employees owe fiduciary duties to employers in addition to their contractual responsibilities.[131] Just as the employer cannot dictate every aspect of an employee's responsibilities in the employment contract, so too the employer's use of employee data cannot be reduced to specific contractual provisions at the outset of the relationship.[132] Given the resulting incompleteness, fiduciary duties are justified to balance out the expectations of the parties and prevent opportunism.[133] The inability of users to competently manage their privacy through notice-and-choice provisions is

---

legal remedy when a private employer discloses true information about its employees to third parties."). Fast has argued that employers should owe a duty of confidentiality to their employees similar to that owed in other fiduciary relationships. Pointing to the sensitivity of employee information on job performance, personal health, and financial records, Fast argued that employers should be considered to have a confidential relationship with their employees. Employers would be liable for disclosing confidential employee information to third parties under a tort theory similar to fiduciary duties. *Id.* at 456-59.

128. RESTATEMENT OF EMP. LAW § 7.05(a) (2015).

129. *Id.* §§ 7.05(b), 7.06.

130. *Id.* § 7.05 cmt. b.

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

132. 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.").

133. *See* Jordan v. Duff & Phelps, Inc., 815 F.2d 429, 438 (7th Cir. 1987) ("Employment creates occasions for opportunism.").

highlighted as a critical reason for assigning fiduciary responsibilities to online service providers.[134] Likewise, individual employees lack the legal understanding and bargaining strength to negotiate for the appropriate level of protections.

Another advantage of approaching the problem of employee privacy loss through a fiduciary framework would be leaving the exact nature of the duties imposed upon employers as information fiduciaries to further development.[135] The theme would be one of protection: employers would be prohibited from using employee data to harm them opportunistically.[136] It is difficult to regulate privacy in the context of employment precisely because there are so many factors to consider with regard to any particular piece of information.[137] But as information fiduciaries, they would have a broader role to play as stewards of the often personal, private, sensitive data that they enmesh in their data collection efforts.

Within this broad relational perspective, it is also possible to sketch out a set of specific obligations that could apply to employers as part of the information fiduciary framework. Here is an initial list of possibilities:

- *A duty of confidentiality*. Long overdue, this duty would require employers to keep their employees' data confidential, even from other employees within

134. Balkin, *supra* note 13, at 17 ("Notice-and-choice models are most inadequate when end users are most vulnerable, and when asymmetries of knowledge, power, and control are greatest."); Richards & Hartzog, *supra* note 32, at 968 (noting the "relative unsophistication of most digital consumers.").

135. *See* Richards & Hartzog, *supra* note 32, at 1013 (stating that "vagueness can be a virtue" in that "[i]ndeterminate obligations help mitigate against companies gaming the system.").

136. *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 30, at 1186 (fiduciaries should "act in ways that do not harm the interests" of those to who they owe fiduciary duties); Richards & Hartzog, *supra* note 32, at 966 (offering a theory "based on the risks of opportunism that arise when people trust others with their personal information and online experiences.").

137. This applies to privacy more generally. *See* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY ix (2008) (arguing that privacy has no single definition but is rather "a plurality of different things."); Katz v. United States, 389 U.S. 347, 360-62 (1967) (Harlan, J., concurring) (basing the constitutionality of a search under the Fourth Amendment on whether a person has a reasonable expectation of privacy).

the company that have no legitimate business reason to have access to it. The duty could be crafted to provide protections similar to HIPAA, with exceptions in cases of specific written consent, legal requirements, or routine business uses.

- *Prohibitions on use of the data for different and unexpected purposes.* Employees often provide sensitive information to employers for very specific reasons, such as requesting accommodations or seeking medical leave. It is opportunistic to then use that information for other purposes, especially without the worker's knowledge and consent.[138]
- *A duty not to profit from the data without employee participation*. Although evidence of this is somewhat murky, some number of companies are selling their employees' data to third parties for independent profit.[139] In many cases, employee data has taken on value independent of its use in managing the employment relationship; The Enron Corpus of employee emails and other interactions was used to generate earlier versions of much of the speech and language AI powering systems today.[140] Uber and Lyft have generated from their drivers an incredibly valuable algorithm of traffic and transportation that has significant independent value.[141] Fiduciary obligations would prohibit employers from selling employee data to third parties without specific consent and a way for employees to participate in the compensation received for the data.

---

138. *Cf.* Richards & Hartzog, *supra* note 32, at 997 (stating that "a duty of loyalty could impose data minimization and purpose limitations that are keyed to the objective, stated purpose for which data was collected.").

139. Adler-Bell & Miller, *supra* note 2, (discussing how corporate employee surveillance "enable[s] 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.").

140. Corinne Purtill, *The emails that brought down Enron still shape our daily lives*, QUARTZ AT WORK (Feb. 15, 2019), https://qz.com/work/1546565/the-emails-that-brought-down-enron-still-shape-our-daily-lives/ [https://perma.cc/E37K-5BH3]; Jessica Leber, *The Immortal Life of the Enron E-Mails*, MIT TECH. REV. (July 2, 2013), https://www.technologyreview.com/2013/07/02/177506/the-immortal-life-of-the-enron-e-mails/ [https://perma.cc/MXP4-WMHN].

141. ALEX ROSENBLAT, UBERLAND: HOW ALGORITHMS ARE REWRITING THE RULES OF WORK 3 (2018).

- *Duties of data security*, *minimization*, *and deletion*. Employers are now increasing data repositories—large reservoirs of information about their employees.[142] Here, Claudia Haupt's comparison to information fiduciaries as trustees is apt, as employers must take on the duty of protecting such a valuable trove from danger.[143] Employers should have a duty of care to implement reasonable data security policies, as well as policies requiring data deletion over time. In terms of the duty of loyalty, a regard for the interests of employees should drive employers to reduce their data collection policies to what is specifically necessary in the context.[144]
- *A duty of obedience to the law*. It may seem anodyne, but a specific requirement to follow the law could bolster efforts to enforce statutory and regulatory requirements provided an independent action for damages were to give it some bite. There is evidence that employers are using surveillance techniques to quash employee organizing;[145] not only does this violate the National Labor Relations Act,[146] but it also seems like an abusive use of monitoring. Moreover, as Richards and Hartzog point out, fiduciary breaches could help establish standing in federal courts for privacy claims.[147]
- *A duty not to harm employees through data collection, use, or disclosure.* A more rigorous approach to the fiduciary relationship, this obligation would ask employers to take the duty of loyalty to employees in the information context seriously. Employers would be prohibited from using data provided by employees to take advantage of them in abusive or inappropriate

142. *See* Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CALIF. L. REV. 241, 244 (2007) ("Computer databases are this century's reservoirs.").

143. *See* Haupt, *supra* note 73, at 37.

144. Richards & Hartzog, *supra* note 32, at 997.

145. Annie Palmer, *How Amazon keeps a close eye on employee activism to head off unions*, CNBC (Oct. 24, 2020, 10:30 AM), https://www.cnbc.com/2020/10/24/how-amazon-prevents-unions-by-surveilling-employee-activism.html.

146. 29 U.S.C. § 158(a)(1); AdvancePierre Foods, Inc. 366 N.L.R.B. 133 (2018).

147. Richards & Hartzog, *supra* note 32, at 1012.

ways.[148] This duty applies more generally in the context of information fiduciaries; in the words of Jack Balkin, "[w]hat information fiduciaries may not do is use the data in unexpected ways to the disadvantage of people who use their services or in ways that violate some other important social norm."[149] To provide a few examples of potentially opportunistic behavior in the employment context: using employee data to manipulate employees without their knowledge; using employee data to build systems that will put the employees out of work, especially if conducted in secret; and disclosing sensitive employee data as a means to harass or punish employees for unrelated offenses.[150]

- *A prohibition on waiver of fiduciary rights.* As a general matter, fiduciary duties are not waivable, and it can be seen as a breach of the duties themselves to ask for them to be waived.[151] This approach should apply to employment, where genuine, uncoerced consent is particularly difficult to establish.

As with other information fiduciaries, the duties of employers to their employees vis-à-vis their data would evolve over time.[152] And as I argued with respect to more general fiduciary obligations for employers, the need for fiduciary responsibilities would diminish if employees were given governance rights.[153] With specific ways to participate in the management of their data—through collective bargaining, works councils, employee board representation, or participatory management systems—workers would be less vulnerable to employer predation. As a result, the need for fiduciary counterbalances would diminish. We are seeing

148. *Cf.* Balkin, *supra* note 30, at 1227 ("[C]onsumers should be able to trust online service providers like Facebook, Uber, or Google not to abuse their ability to collect and use personal information for profit.").

149. *Id.*

150. *Cf. id.* ("It should be reasonable to expect that a transportation broker or an online dating service will not attempt or threaten to embarrass you to keep you from criticizing it. It is also reasonable to expect that a social networking service is designed to facilitate social networking and not to manipulate you into voting for the candidate of its choice because it wants to rig an election.").

151. Richards & Hartzog, *supra* note 32, at 998.

152. *Id.* at 1013.

153. Bodie, *supra* note 114, at 867.

increasing calls for governance rights for users of online services to combat their vulnerability.[154] Similarly, such governance rights might ultimately be the best approach within employment.

IV. CONCLUSION

In making the case that online service providers should be considered information fiduciaries, Jack Balkin stated: "Fiduciary obligations arise from social relations of unequal power and vulnerability."[155] The employment relationship has traditionally been considered one of unequal power and vulnerability; new techniques for gathering, using, and disclosing employee data have only amplified this disparity. Requiring employers to live up to their responsibilities as information fiduciaries would help to mitigate this power imbalance and discourage employers from taking full and unfair advantage of their powers. It may be only one of the steps necessary in this new data-rich environment, but it is one worth taking.

154. *See, e.g.*, Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 1598, 1601-02 (2018); Salomé Viljoen, *A Relational Theory of Data Governance*, 131 YALE L.J. 573, 577-78 (2021).

155. Balkin, *supra* note 13, at 25-26.