Scholedge International Journal of *Business Policy & Governance*
ISSN 2394-3351 Vol. 13, Issue 01 (2026)
DOI: https://dx.doi.org/10.19085/sijbpg130102

Digital Platforms, Data Sovereignty, and Corporate Power: Rethinking Governance in the Platform Economy

Satish Kumar
SKS Consulting & Advisors, India

ABSTRACT

Digital platforms have redrawn the boundaries of economic power, public trust, and data control in ways that most regulatory frameworks were not designed to handle. This paper examines how platform giants accumulate and exercise corporate power, why data sovereignty has become a contested terrain, and where trust deficits emerge in organizational settings that depend on these platforms. Drawing on existing literature in platform studies, political economy, and digital governance, the paper maps the structural conditions that make platform overreach possible. It then presents documented cases in which platform-enabled practices eroded trust within workplaces and among users. The paper closes with practical advisories for workplace managers who must operate within, and alongside, platforms whose interests do not always align with those of the people they serve.

Keywords: Platform economy, data sovereignty, corporate power, digital governance, workplace trust, algorithmic management

INTRODUCTION

The word 'platform' once described a physical stage. Today it describes something far more consequential: a digital infrastructure that connects buyers and sellers, employers and workers, publishers and audiences, and that extracts data from every transaction along the way. Companies like Google, Amazon, Meta, Apple, and Microsoft collectively govern much of the world's digital communication, commerce, and work. Their power rests not on armies or raw materials but on data, algorithms, and network effects that reinforce themselves the more people use the system.

This concentration of power raises questions that scholars, regulators, and organizational managers cannot defer indefinitely. Who owns the data generated by users and workers on these platforms? What happens when platform interests conflict with those of the organizations that depend on them? And when trust breaks down—between employers and workers, between platforms and users—what tools do managers have to repair or contain the damage?

This paper takes those questions seriously. It reviews what researchers have established about platform economics and data governance, identifies documented cases where trust deficits have appeared in platform-dependent workplaces, and then offers concrete advisories for managers navigating this landscape. The goal is not to condemn platforms wholesale but to be clear-eyed about the structural conditions they create and the practical steps that managers can take in response.

THE ARCHITECTURE OF PLATFORM POWER

Platforms are not simply software. They are, as Srnicek (2017) describes them, a specific business model that positions itself as an intermediary between two or more sides of a market, then monetizes the interactions it facilitates. The logic is elegant and, for platform owners, enormously profitable: the platform rarely owns the goods being exchanged. Uber owns no taxis. Airbnb owns no apartments. Meta creates almost no content. What they own is the infrastructure through which exchange happens, and in owning that infrastructure, they capture vast amounts of behavioral data.

Parker et al. (2016) explained the power of this model through network effects. The more participants a platform attracts, the more valuable it becomes to each participant, which in turn attracts more participants. This self-reinforcing dynamic creates what economists call winner-take-most markets, where one or two dominant platforms crowd out competitors and become near-impossible to dislodge. Once a platform reaches a certain scale, the practical cost of switching to an alternative becomes prohibitively high for most users and organizations.

Van Dijck et al. (2018) extended this analysis by showing that platforms are not merely economic actors. They shape public discourse, influence what information people see, and encode values into their design choices. When a platform decides what content to amplify, which workers to dispatch, or what prices to set, it is making decisions that were once made by human managers, editors, or market mechanisms. These are governance decisions, even when they do not present themselves as such.

Zuboff (2019) coined the term 'surveillance capitalism' to describe the economic logic underlying this architecture. Platforms collect behavioral data, process it through predictive models, and sell access to those predictions to advertisers and other buyers. In this logic, human experience is a raw material, and the surplus extracted from it fuels the platform's commercial dominance. Zuboff's critique extends beyond privacy. It is ultimately about power: the power to predict and modify behavior at scale, without the knowledge or meaningful consent of those being observed.

DATA SOVEREIGNTY AND THE STRUGGLE FOR CONTROL

Data sovereignty is the principle that individuals, organizations, or states should have meaningful control over data generated within their jurisdiction or about their activities. The concept is straightforward in the abstract but fiercely contested in practice.

The European Union's General Data Protection Regulation (GDPR), which came into force in May 2018, represents the most ambitious legislative attempt to operationalize data sovereignty at scale (European Union, 2016). GDPR established rights for individuals to access, correct, and delete personal data held about them, and placed obligations on organizations handling that data. Fines for non-compliance can reach four percent of global annual turnover. The regulation made a clear statement: data protection is a fundamental right, not a tradeable commodity.

Yet GDPR has not resolved the underlying tensions. Platforms with global reach can shift data processing to jurisdictions with weaker protections. The consent mechanisms built into most platform designs are widely regarded as inadequate, because users face a binary choice between accepting data collection and forgoing the service entirely (Couldry & Mejias, 2019). That is not genuine consent; it is a forced bargain. When the only alternative to accepting surveillance is to be excluded from a near-essential service, the concept of voluntary agreement loses most of its meaning.

For organizations, data sovereignty has additional dimensions. When a company adopts a platform-based tool—a cloud storage service, a productivity suite, a communications platform—it typically transfers significant control over its data to the platform provider. The platform's terms of service determine how that data is used, who can access it, and what happens to it if the relationship ends. Many organizations sign these terms without fully reading them, let alone negotiating them, which means they often have little idea what rights they have surrendered.

CORPORATE POWER AND THE CONDITIONS FOR TRUST DEFICITS

Trust in organizational settings depends on predictability, transparency, and a sense that power is exercised in ways that are fair and accountable. Platforms, by their nature, disturb all three of those conditions.

Predictability suffers because platform operators change their algorithms, policies, and pricing without notice. A business that built its customer acquisition strategy around organic reach on a social media platform can find that strategy worthless overnight when the platform adjusts its algorithm. A worker who depended on an app-based gig economy platform for income can find their account suspended without clear explanation or meaningful appeal. These are not edge cases; they are recurring features of platform-mediated economic relationships.

Transparency suffers because the algorithmic systems that govern platform behavior are, in most cases, proprietary and opaque. Managers, workers, and users interact with outputs—recommendations, scores, rankings—without understanding how those outputs were produced or what assumptions are embedded in the models behind them.

Accountability suffers because platforms operate across jurisdictions and organizational boundaries in ways that make it difficult to assign responsibility when things go wrong. When a platform's recommendation algorithm amplifies misinformation, or when its data practices expose user information to unauthorized third parties, the question of who is responsible rarely has a clean answer.

Balkin (2016) argued that this combination of scale and opacity creates a new category of institutional actor that should be subject to fiduciary obligations—duties of loyalty and care toward the people who depend on them—rather than simply the contract terms platforms draft for themselves. This argument has not yet translated into law in most jurisdictions, but it captures something important about the structural imbalance between platforms and those who rely on them. The platform writes the rules; the user or organization agrees to them or opts out entirely.

Flew (2021) reinforced this point by noting that existing regulatory frameworks were designed for a world in which market actors, employers, and service providers were more clearly defined and more geographically bounded. Platform companies fit awkwardly into those categories, which is one reason they have been so effective at outrunning regulation.

REAL-WORLD CASES WHERE TRUST DEFICITS EMERGED

Facebook and Cambridge Analytica (2018)

In 2018, it emerged that Cambridge Analytica, a political consulting firm, had harvested personal data from approximately 87 million Facebook users without their explicit consent. The data was collected through a third-party application that exploited Facebook's then-permissive API policies, which allowed apps to collect not only data about their own users but also about those users' Facebook friends. The scale of the exposure—and the fact that it was used for political targeting—made the episode one of the most damaging corporate data scandals in recent memory.

The consequences were extensive: congressional hearings, regulatory investigations across multiple continents, a $5 billion fine from the US Federal Trade Commission, and a sharp collapse in user trust. For organizations that had integrated Facebook's tools into their marketing and communications operations, the episode raised uncomfortable questions about how much they actually knew about the data practices of the platforms they depended on. Many found the answer was: very little.

The workplace dimension of the Cambridge Analytica case was the exposure of how organizational reliance on a platform's data infrastructure can create liability and reputational risk that the organization cannot fully control. The data was Facebook's to manage or mismanage; the trust damage fell partly on the organizations that had built operations around Facebook's ecosystem. That dependency had been convenient, but its costs became visible in the worst possible way.

Amazon's Warehouse Surveillance

Amazon's use of algorithmic management in its fulfillment centers has been documented by journalists and labor researchers. Workers in these facilities are tracked continuously: their movement, productivity rates, idle time, and in some reported cases, even the time they spend away from their stations has been monitored and fed into systems that generate warnings and, eventually, terminations. Reporting by major news outlets has described workers who felt unable to slow their pace even when injured, because they feared the system would flag their productivity drop.

When management is mediated entirely by an algorithm, the human relationship between a worker and a supervisor can effectively disappear. There is no one to explain the score to, no one to whom a worker can describe the circumstances behind a slow hour, and no one with the authority or inclination to exercise judgment. The system knows the output but not the inputs, and it is not designed to ask.

This is a trust deficit in a specific and serious sense. Workers cannot trust that they will be evaluated by someone who understands context. The result, as documented in the literature on algorithmic management, is not simply dissatisfaction but a breakdown of the psychological contract between employer and worker—the unwritten understanding that work performed in good faith will be assessed in good faith (van Dijck et al., 2018).

Uber and the Algorithmic Management of Gig Workers

Uber's relationship with its drivers illustrates a different dimension of the same problem. Drivers are classified as independent contractors rather than employees in most jurisdictions, which exempts Uber from many of the legal obligations that govern employment relationships. At the same time, drivers are subject to algorithmic control that determines which trips they receive, what dynamic pricing they earn, and whether their accounts remain active.

When a driver's rating falls below a threshold, their account can be deactivated with limited explanation and without a meaningful grievance process. Van Dijck et al. (2018) described this dynamic as platform governance—the exercise of authority through design and algorithm rather than through employment contracts or regulatory frameworks. The legal fiction of independence coexists with operational control that functions very much like employment, but without any of the protections.

For drivers, the trust deficit is acute. They are economically dependent on a system they do not control, subject to decisions they cannot interrogate, and without the institutional protections that employees ordinarily possess. For other organizations watching this model, the lesson is that platform dependency can strip away accountability mechanisms that those organizations had previously taken for granted.

Google Workspace and Enterprise Data Concerns

Google Workspace is used by millions of organizations as their primary productivity platform. Google's contractual commitments to enterprise customers are substantially stronger than its terms for individual consumers, and the company has stated that it does not use enterprise customer data for advertising purposes. However, the architecture of the system still means that organizational communications, documents, and strategic plans are stored on infrastructure that Google controls.

For organizations operating in sensitive sectors—legal, medical, financial, governmental—this creates a governance question that cannot be answered solely by reference to Google's current conduct. The question is not just what the platform does now, but what it could do under different ownership, different leadership, or a different legal environment. Trust is not simply a matter of past behavior; it is also a matter of structural dependency and what it enables. The question is not whether Google has behaved well, but what the organization's position would be if it did not.

GOVERNANCE FRAMEWORKS: EXISTING TOOLS AND THEIR LIMITS

The governance frameworks that exist for platform oversight fall into roughly three categories: data protection regulation, competition law, and sector-specific oversight. None of them fully addresses the conditions described in the previous sections.

Data protection regulation, exemplified by GDPR, focuses on information rights and consent. It gives individuals tools to know what is collected about them and to request its deletion. It does not directly address the power imbalance between platforms and the organizations that depend on them, and it has struggled to keep pace with the speed at which platform technologies evolve and the sophistication with which platform companies structure their legal and technical operations to minimize liability.

Competition law has been increasingly applied to platform markets, with antitrust actions brought against Google, Meta, Apple, and Amazon in the United States and Europe recently. These actions address market dominance and anti-competitive conduct. But antitrust remedies work slowly, often taking years from investigation to enforcement, and the underlying conditions they seek to correct—winner-take-most markets, network effects—are structural features of the platform model rather than simply the result of identifiable bad acts.

Flew (2021) noted that effective platform governance requires coordination across agencies and jurisdictions, something that has proven extremely difficult in practice. Platforms operate globally while most regulatory authority remains national. This mismatch is not accidental. Platform companies have consistently lobbied against harmonized international regulation and have structured their operations across jurisdictions in ways that maximize that mismatch's advantages for them.

Couldry and Mejias (2019) framed the problem in broader terms, arguing that what they call 'data colonialism'—the extraction of value from human behavior at scale—represents a structural condition that individual regulatory interventions are unlikely to reverse. They are probably right that no single regulatory move will resolve the underlying dynamics. But that does not mean that nothing can be done, especially at the organizational level.

ADVISORIES FOR WORKPLACE MANAGERS

The structural problems of platform power and data sovereignty are real, and most workplace managers cannot solve them independently. But there is a meaningful gap between what managers cannot control and what they simply have not thought carefully about. The advisories below are aimed at that gap. They are practical and proportionate, and most organizations can implement them without significant external investment.

MAP YOUR PLATFORM DEPENDENCIES

Most organizations cannot tell you, without some research, exactly which platforms hold their data, what the terms of those relationships are, or what would happen if any one platform became unavailable or changed its terms materially. Start there. Build a platform dependency inventory that lists every major platform tool in use, what data it holds or processes, and what the termination and data export options are.

This is not a complicated exercise technically, but it requires someone to own it. Assign it. Review the results with leadership. The inventory will likely surface relationships that are more fragile, and more data-laden, than anyone realized. Many organizations discover at this stage that they have signed terms they have never read, for tools handling data they had not realized the platform was collecting.

Assign a named person or team—an IT lead, a compliance officer, or a senior manager—to build the inventory within 60 days. Use a simple spreadsheet. The goal is visibility, not perfection. Once the picture is clear, leadership can decide what to do about it.

READ THE TERMS—OR PAY SOMEONE WHO WILL

Platform terms of service are long, written in dense legal language, and designed to be agreed to without being read. Most organizations sign them without reading them. This is a governance failure, and it is correctable.

For any platform that holds significant organizational data or that workers depend on for their livelihood, the terms should be reviewed by someone who understands what they mean. This does not require outside counsel for every tool, but it does mean training an internal person to evaluate key clauses related to data use, data export, termination rights, and liability.

Create a tiered review process. Tier 1 covers high-data, mission-critical platforms and requires a full legal review of terms before signing and at each renewal. Tier 2 covers tools with moderate data exposure and calls for internal review of key clauses. Tier 3 covers low-data, commodity tools and needs only a standard procurement checklist. The tiers can be defined in a day; building the habit takes slightly longer but is not complicated.

SET LIMITS ON ALGORITHMIC MANAGEMENT

If your organization uses platform-based tools to manage workers—productivity tracking, algorithmic scheduling, performance scoring—think carefully about what those systems are actually measuring and what they are missing. The documented cases from Amazon's warehouses show what happens when algorithmic management operates without human judgment as a check: workers are evaluated on outputs alone, stripped of context, and without any meaningful way to contest the result.

Workers need to know what is being measured and why. They need access to their own performance data. They need a human escalation path when they believe an automated result is incorrect or unfair. None of these things require large investments, but all of them require a conscious decision that they matter.

Audit every automated performance or management tool currently in use. For each, document what data it collects, how it produces its outputs, who reviews those outputs before decisions are made, and what a worker's right to contest a decision looks like. Where the answers are inadequate, fix them before the next performance cycle.

BUILD DATA MINIMIZATION INTO PROCUREMENT

When evaluating a new platform tool, data minimization should be a procurement criterion alongside cost and functionality. The question is not simply 'does this tool do the job?' but 'does this tool collect more data than the job requires?' Choosing tools that collect less, or that offer meaningful controls over data use, reduces organizational exposure and sends a signal to workers and clients that the organization takes their data seriously.

Add data minimization criteria to your standard procurement checklist. Ask vendors directly: what data does this tool collect, where is it stored, who has access to it, and how is it deleted when we terminate the relationship? Treat inadequate answers as a serious procurement risk, not a minor administrative gap.

COMMUNICATE OPENLY ABOUT PLATFORM USE

Trust between employers and workers depends partly on workers knowing what tools are in use and how those tools affect them. In many organizations, monitoring and tracking tools are deployed with little or no notice to workers. This may be legally permissible in many jurisdictions, but it is not a good foundation for trust.

Managers who communicate openly about what tools are in use, what data they collect, and how that data is used in employment decisions are much less likely to face the kind of trust collapse that comes when workers discover surveillance they did not know about. The Cambridge Analytica episode was damaging partly because of what Facebook did, but at least as much because users learned about it from journalists rather than from Facebook. Discovery through third parties is almost always more damaging than disclosure by the organization itself.

Develop a clear, plain-language policy describing what monitoring and data collection tools are in use, what they collect, and how that information figures in employment decisions. Share it with all workers at onboarding and whenever new tools are added. Review it annually.

DIVERSIFY WHERE POSSIBLE

Platform lock-in is a genuine organizational risk. Organizations that have concentrated their operations around a single platform are vulnerable if that platform changes its terms, raises its prices, experiences a major outage, or becomes unavailable for regulatory reasons. Where genuine alternatives exist, diversifying platform relationships reduces this vulnerability.

This is not always cost-effective. Some platforms are near-essential infrastructure, and the switching costs are real. But the short-term convenience of deep platform integration is worth weighing consciously against the long-term risk of dependency. Many organizations have made this trade-off without realizing they were making it.

Identify your three highest-dependency platform relationships. For each, assess the realistic cost of switching and the availability of credible alternatives. Make a conscious decision about whether to accept the dependency or invest in reducing it, and document that decision. Revisit it every two years, or whenever a platform makes a significant change to its terms or pricing.

CONCLUSION

The platform economy is not going anywhere. The concentration of data, infrastructure, and market power in a small number of digital platforms is a structural feature of the current economic landscape. For workplace managers, this means learning to operate in an environment where important decisions about data, labor, and organizational infrastructure are shaped by actors whose interests do not always coincide with theirs.

The cases examined in this paper—Facebook's data practices and Cambridge Analytica, Amazon's warehouse surveillance, Uber's algorithmic management of gig workers, and Google's enterprise data architecture—show that trust deficits in platform-dependent workplaces are neither hypothetical nor rare. They are documented, recurring, and consequential. They damage relationships between employers and workers, between organizations and their clients, and between platforms and the public that increasingly depends on them.

Governance responses at the regulatory level are real but uneven, and they operate on timelines that offer little comfort to managers dealing with problems today. The advisories offered here are not a substitute for better regulation; they are a response to the conditions that exist right now. Mapping platform dependencies, reading and negotiating terms, setting limits on algorithmic management, building data minimization into procurement decisions, communicating openly with workers about monitoring, and diversifying platform relationships where possible—none of these actions solve the structural problem. But together, they reduce exposure, improve transparency, and preserve the basic conditions under which trust between workers and organizations can be maintained.

The platform economy creates real risks for organizations willing to look at them clearly. Most of the practical responses are within reach. The main requirement is the decision to take them seriously.

REFERENCES

Balkin, J. M. (2016). Information fiduciaries and the First Amendment. *UC Davis Law Review*, *49*(4), 1183–1234.

Couldry, N., & Mejias, U. A. (2019). *The costs of connection: How data is colonizing human life and appropriating it for capitalism*. Stanford University Press.

European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data*. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Flew, T. (2021). *Regulating platforms*. Polity Press.

Parker, G. G., Van Alstyne, M. W., & Choudary, S. P. (2016). *Platform revolution: How networked markets are transforming the economy and how to make them work for you*. W. W. Norton & Company.

Srnicek, N. (2017). *Platform capitalism*. Polity Press.

van Dijck, J., Poell, T., & de Waal, M. (2018). *The platform society: Public values in a connective world*. Oxford University Press.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.