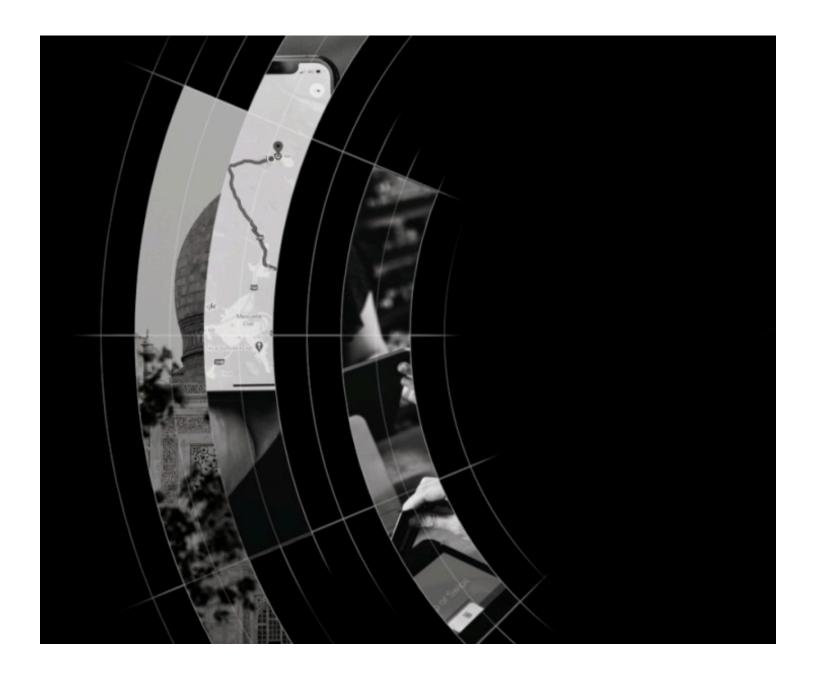# LOGIC(S)

Issues   Donate   Store   Subscribe   About

Subscribe by May 17 to receive the first issue of the relaunched, groundbreaking Logic(s) Magazine

ISSUE 13 / DISTRIBUTION

MAY 17, 2021

Data Relations

Salomé Viljoen

What's wrong with our digital world? What would make it right?

For almost as long as there have been digital technologies, there have been critiques of digital technologies. One of the oldest and most consistent concerns associated with computation is "datafication." Datafication turns the activity of people online (and, increasingly, offline) into data, that all-important resource that allows companies to discover patterns in our behavior and exploit them for commercial gain.

Consider a simple example. If I walk into the café across the street and buy a coffee using the store's Square payment system, this transaction is datafied. Information about what kind of coffee I bought, how much I paid, and what time I bought it is gathered by Square and added to the dossier of all my past purchases and the dossier of all the café's past sales. By datafying this transaction, Square can learn about my consumption patterns and about the café's business. Square may then use these lessons for commercial gain: for instance, by selling information about coffee purchasing activity in my neighborhood, or by developing risk profiles for commercial loans to coffee shops.

Datafication is a basic part of what makes the digital economy digital; it also features prominently in critiques of the digital economy. But what makes datafication wrong, exactly? Currently, there are two main lines of thought. First, datafication is a form of surveillance that violates our autonomy by undermining the ways in which we develop our sense of ourselves and express those selves in the world. Second, datafication is like feudalism—it traps us in unfair economic arrangements in which we provide our valuable "data assets" or

"data work" for free by using the digital services created by tech companies.

Both of these perspectives provide valuable insights into why we should care about datafication. Yet they also have serious limitations. In the digital economy, data isn't collected solely because of what it reveals about us as individuals. Rather, data is valuable primarily because of how it can be aggregated and processed to reveal things (and inform actions) about groups of people. Datafication, in other words, is a social process, not a personal one. Further, it is a process that operates through a set of relationships. Only by highlighting the collective and relational character of datafication can we understand how it works, and the particular injustices that it produces. This isn't just a theoretical exercise—it goes to the heart of what's wrong with our digital world, and what may make it right.

Autoplay in the Panopticon

Traditionally, critiques of datafication have focused on the kinds of violations we identify with surveillance. This suggests datafication is wrong because it violates our "right to be let alone," to quote Louis Brandeis, the father of US privacy law. Surveillance is a fundamental transgression because it undermines our ability to form autonomous selves.

This account of what makes datafication wrong has its popular origins in Michel Foucault's analysis of the panopticon. The original panopticon was a blueprint designed by the eighteenth-century philosopher Jeremy Bentham. It consisted of a cylindrical prison with a guard tower in the central courtyard. The prisoners could only see the guard tower, while the guard had a view into every prisoner's cell. While this model was never adopted during Bentham's lifetime, Foucault used the panopticon as a metaphor for the "political technology" that undergirds the modern disciplinary society. The panopticon's design structures a relation of power through surveillance: an "unequal gaze" between the all-seeing observer and the observed.

In this view, surveillance, whether it takes the form of a prison or a dataflow, makes subjects legible to observers, and therefore more controllable. In the panopticon, the prisoner never knows for sure if she is being watched. So she must assume she is, with the result that she begins to police her own behavior and to internalize the goals of the prison guard as her own. In other words, surveillance technologies don't just observe us. They can also change how we act.

Foucault was primarily interested in how the state used surveillance to produce docile and predictable citizens. More recently, however, large tech firms have been using surveillance to produce predictable and profitable consumers. Netflix's autoplay feature is a good example. For Netflix, one of the most important indicators of user engagement—and, by proxy, customer satisfaction—is watch time: how many hours someone spends on the site. In order to maximize watch time, Netflix ran a series of tests that involved tweaking its interface in various ways to see which changes resulted in more watch time from its users. These tests showed that the best way to increase user engagement was to automatically begin playing the next episode. Netflix's granular, data-intensive analysis even suggested the most effective "wait time" before the next episode played: seven seconds.

Through surveillance, Netflix has found a way to modify TV-watching behavior with its own goals in mind. The site nudges a user into doing something that feels good in the moment, but that may go against her better judgment and her own will, if only she had a few seconds more to think about it.

Strengthening privacy rules could mitigate such concerns. Such rules might require companies to obtain meaningful (not coerced) consent or give data subjects more control over how their data is used. These expanded rights would reassert the authority of the individual's will against the manipulative machinations of technology companies, restoring the autonomy that has been destroyed by datafication.

Show Me the Money

Datafication doesn't just involve observing and manipulating individuals, however. It also involves monetizing the data that is collected from them. This brings us to another critique of datafication. If one camp argues that surveillance erodes our autonomy, another emphasizes the unfairness of companies getting rich from our data. The same techniques that influence user behavior also generate wealth for tech companies, thus contributing to growing economic inequality. The data-intensive practices of companies like Google, Amazon, and Facebook have made them and their CEOs fabulously rich, in great part due to how these companies exploit the insights they can gain from their vast stores of user data.

One solution is to pay people for their data. If datafication is wrong because of how it helps companies make money from users without compensating them, then forcing those companies to compensate their users could right this wrong. Gavin Newsom, Andrew Yang, and Alexandria Ocasio-Cortez have all expressed support for the idea. And the proposal gets at something crucial about datafication missing from the surveillance-centered critique: the stark distributive realities of the digital economy.

The pandemic has brought unemployment and hardship to many but has been a boon to tech monopolies. Jeff Bezos' wealth grew by more than $70 billion in 2020. Paying people for the data they supply to tech companies is one way to recapture and redistribute some of this prosperity. It would spread the wealth made through datafication more evenly among all of those who helped create it.

Relations, Not Things

Both the "autonomy" and the "nonpayment" accounts of datafication make valuable points. But they also miss essential aspects of how datafication works and what makes it wrong. It's true that datafication can impede our free will. However, an emphasis on personal autonomy can obscure the extent to which the stakes of data collection extend far beyond the individual data subject. It's equally true that datafication contributes to inequality. But paying individuals for their data won't eliminate that inequality because it doesn't address the broader conditions that can make datafication coercive.

In an increasingly digital world, datafication is the material process whereby a great deal of injustice happens. Through datafication, we are drafted into the project of one another's oppression. This is not a personal process, but a social one. Datafication operates through a set of relationships. There are the relationships between us and the executives and investors who enrich themselves by surveilling us. There are also the relationships inscribed by racism, sexism, xenophobia, and other group-based oppressions, which datafication manifests in new digital forms.

These "data relations" are the digital expression of the growing gap between tech's winners and losers: those who predominantly benefit from datafication's personalization and efficiency, and those who disproportionately bear its risks. Sometimes these gaps are economic, like those between platform CEOs and the gig workers who make them rich. Other times they are social, like those between Amazon Ring homeowners who enjoy being able to make sure their packages are safe, and passersby that the Ring subjects to heightened risk of violent police encounters. In both cases, data relations materialize relationships of domination between different groups of people.

A recent story by Joseph Cox for *Vice* offers an especially dramatic example of this dynamic. According to Cox's reporting, the US military is purchasing granular location data from a popular Muslim prayer app with over 98 million downloads worldwide. The app, Muslim Pro, pings its users five times a day with reminders to pray, uses a compass to orient them toward

the Kaaba in Mecca, helps them observe fasting during Ramadan, and guides them to halal food in their area. These features have helped turned Muslim Pro into the most popular Muslim app in the world, according to its maker, Bitsmedia. It has also meant that the app collects vast quantities of detailed location data.

The revelation that this data is now in the hands of the US military has sparked dismay and condemnation in the Muslim community. But what makes this instance of datafication wrong? Under the autonomy account, the dataflow from a user to Muslim Pro to the US military is wrong because the user is being surveilled by a government whose presence in their religious life may have a chilling effect on their religious activities. Had the user been notified or given the option to opt out of this sale, they would almost certainly have done so. Under the nonpayment account, on the other hand, this dataflow is wrong because users are not being paid by the app or the US military for their data. If the sale of user data is making Muslim Pro money, users deserve some portion of that profit.

Both of these analyses may be partially true, but both are unsatisfactory. Imam Omar Suleiman, a prominent Muslim scholar and the founder of Yaqeen Institute for Islamic Research, highlights the importance of the broader social and historical context for understanding what makes the Muslim Pro situation particularly harmful. "This is not taking place in a vacuum," Suleiman told the *Los Angeles Times*. He notes the long pattern of government "violations of our civil liberties that have preyed on our most basic functions as Muslims"—a pattern that includes not only intensive domestic surveillance, but also the expansion of the drone program under President Obama, which resulted in hundreds of civilian deaths in Muslim-majority countries.

The responses from Muslim community leaders reflect the social—not merely individual— significance of the dataflow between Muslim Pro and the US military. For them, this instance of datafication is wrong because it drafts users—faithful Muslims—into the project of their fellow Muslims' oppression. It takes a digital means for expressing and enacting their faith

and transforms it into a vector for potential violence, materializing the imperial relation between Muslims and the US state. Datafication is a fundamentally collective and relational process, and so are the injustices that it inflicts.

Asking the Right Questions

Defining datafication in this way doesn't just present us with a more complete picture of how the process works. It also gives us a way to make datafication more just. Like analog social relations, our data relations may be oppressive, exploitative, and even violent. But also like analog social relations, our data relations may be empowering and supportive and may act as a moral magnifier—enabling us to achieve goals together that we could not accomplish alone.

Thinking of datafication as the digital terms by which we relate to one another clarifies the kind of political interventions that are required. The point is not to define the terms of our individual datafication—by demanding our share of the pie, or shoring up resistance to being rendered legible against our will—but to define the terms of our collective datafication. We may choose to define those terms in ways that contribute to greater equality. For instance, we might apply datafication toward retrieving spheres of life from market governance. Aaron Benanav has described the role that digital infrastructures could play in democratizing production and allocation decisions by substituting the information generated through datafication for price signals. Other urgent public tasks may also require datafication. A detailed accounting of our individual and collective use of natural resources will be increasingly necessary for the efficient and fair allocation of these resources as our environment undergoes accelerating climate change.

What kinds of projects are worth being drafted into? What forms of relating to one another are just? And how do we begin to develop the institutions through which the democratic

negotiations of our shared priorities can be facilitated? A theory of what makes datafication wrong can't provide us with the substantive, and essentially political, answers to those questions. But it can clarify which questions need answering in order to achieve a more democratic future.

SALOMÉ VILJOEN IS A JOINT RESEARCH FELLOW AT NEW YORK UNIVERSITY SCHOOL OF LAW and Cornell Tech studying the legal theory of data governance.

This piece appears in *Logic*'s issue 13, "Distribution". To order the issue, head on over to our store. To receive future issues, subscribe.

The mission of Logic(s) is to draw in voices and perspectives that remain outside, underexplored, and essential to thinking critically about technology from below.

Logic(s) Magazine
Email Us

Stay connected with us for news, events, and more.

email address   Sign up