2025

Reimagining AI

For Environmental Justice and Creativity

COLLECTION OF ESSAYS

Edited by:
Jess Reia I MC Forelle I Yingchong Wang

VERIFIED HUMAN?
Identity Inversions in Our New Machine Age

Aaron Martin

Department of Media Studies and School of Data Science

University of Virginia

Keren Weitzberg

School of Politics and International Relations, Institute for the Humanities and Social Sciences

Queen Mary University of London

In a world overrun by bots and AI agents, afflicted by automated disinformation, fraud and scams, and struggling to cope with an onslaught of machine-generated "slop," many worry about how we can ensure meaningful human exchange and prosperity in the future. Some have called for restrictions, a pause, or even a moratorium on AI, but for others, these technology-exacerbated problems necessitate a technology-enabled solution, namely biometrics: the automated measurement and recognition of our physical characteristics or behaviors. Specifically, it is argued that to ensure a trustworthy digital economy in which AI is ubiquitous, more and more of our interactions and transactions will soon necessitate strong forms of human identification and authentication based on biometrics. Probably one of the most extreme (and polarizing) advocates of such a view is Worldcoin (now rebranded as World), a project from the company Tools for Humanity (TfH). Co-founded by OpenAI's Sam Altman, TfH's World has biometrically registered millions of people across countries like Indonesia, Chile, and Kenya and is aggressively trying to expand its operations globally despite sustained regulatory pushback largely on privacy and data protection grounds.

Critically, through developments like these, we are witnessing an important shift in the purported objectives of the technologies of biometrics. Once intended as a technical means to assign "uniqueness" to people by distinguishing one person from another, biometrics are now being resignified as technologies for assuring humanness—distinguishing us from bots. TfH's World project, for example, anticipates a future in which humans are indistinguishable

from AI absent frequent biometric checks, and ordinary people have been rendered unemployed by computers, making it necessary to distribute a biometrically controlled universal basic income. How worried should we be about such a prospective future?

For sure, the signs of AI's degenerative effects on our societies are all around us: bots are everywhere and spreading—they are scraping the web, providing customer "service," polluting social media, and so on. Across a growing number of different sectors, automated agents[41] are being deployed to augment or in some cases replace the work of humans. Many fret about what this invasion means for online discourse and digital interactions, as well as for the quality and sustainability of our societies and politics.

In certain jurisdictions, regulators are beginning to intervene. Some are imposing transparency requirements on bot operators to make it clearer when we are interacting with a machine. However, this requires the goodwill of whomever is deploying bots. In other cases, regulators are forcing platforms to more proactively detect and remove "inauthentic" activity. The EU's Digital Services Act, for example, includes strong requirements to prevent intentional manipulation by bots. But these are only partial measures—the problem of AI and identity assurance is much bigger than a platform regulation issue. It cuts across a wide range of domains. For example, the humanitarian sector (where our research[42] is largely focused) is reflecting on the implications of AI on the potential risks of beneficiary "fraud". In a sector with notoriously weak identity management, the increasing digitization of aid, most notably humanitarian cash assistance, could be severely challenged by the misuse of AI to create false identities. Is more extensive use of biometrics the solution?

For well over a century, biometric technologies have been aimed at eliminating "fraud" through authentication, verification, and deduplication (i.e. finding people who are registered in a system or database using multiple different identities and deactivating duplicative data), using supposedly unique bodily characteristics, such as fingerprints or iris scans, to detect fraudsters. But the emergence of "synthetic identities" (which combine real and fake information to create a new identity that does not correspond to any real person) is pushing the boundaries of these technologies and imagining their use to new ends.

Companies like TfH's World claim to have the solution to these problems, i.e. a biometrically-enabled "proof of personhood."[43] Their sales pitch suggests that we can reclaim our digital sovereignty—and even our humanity—by relinquishing our data to them. In this radically libertarian and dystopian scenario in which a private company, not the state, is designated to provide a critical infrastructure, biometrics assume a new ontology (from individuating humans to distinguishing machines). Such a scenario invites the use of a surveillance technology that will no doubt encroach on different domains of social, economic, and political life. It also reduces humanness to a technical protocol for proving personhood—something that we ought to resist, no matter who is involved.