The AI Human Condition is a Dilemma between Authenticity and Freedom

Abstract
Big data and predictive analytics applied to economic life is forcing individuals to choose between authenticity and freedom. The fact of the choice cuts philosophy away from the traditional understanding of the two values as entwined. This essay describes why the split is happening, how new conceptions of authenticity and freedom are rising, and the human experience of the dilemma between them. Also, this essay participates in recent philosophical intersections with Shoshana Zuboff's work on surveillance capitalism, but the investigation connects on the individual, ethical level as opposed to the more prevalent social and political interaction.

Keywords
authenticity, freedom, personal identity, artificial intelligence, surveillance capitalism

Words
2510

There is an impending dilemma between authenticity and freedom. It's not clear whether one or the other will be preferable, but the indecision is critical because it ruptures the history of philosophy and ethics. From Kierkegaard to Heidegger, the pursuit of authenticity has been the reason for, and proper expression of personal freedom: the two have been entwined (Menke 2005: 308). Today, I argue, big data technology and predictive analytics are forcing them apart, and so opening new ethical uncertainties. These dilemmas, I conclude, delineate the nascent AI human condition.

First, the particular authenticity that artificial intelligence reality produces, especially on the economic level, will be sketched. Then, the opposing freedom will be described as an expression of inauthenticity.

Exposure of my personal information

A key to authenticity is personal transparency in the sense of seeing ourselves without reservation (Guignon 2004: viii).

This transparency is beginning to happen today. To start, there is camera and microphone proliferation. Increasingly they monitor our homes, streets and workplaces, and with a constantly widening view to include facial micro-expressions and the tones of our voices (Takalkar et al 2018). Then there are memories – those we want to keep and the ones we try to forget – gathered by social media platforms. Wearables track who we are biologically (Voas & Kshetri 2017). Subtle patterns discernable only through big data filtering indicate urges and fears, and consequently what's most disconcerting about transparency may not be what others see in us, but what we see in ourselves. More could be added, but this is enough to mark the trajectory of the advancing technology toward personal exposure.

When the monitoring technology is fueled by economic profit, Shoshana Zuboff perceives the emergence of a new kind of capitalism, centering on surveillance (Zuboff 2015: 76). As she describes, being rendered transparent –

informationally nude – can lead to revolting consumer manipulation (Zuboff 2019). But she's less sensitive to, or at least less prone to report, this: there is also something enticing. If revealing our most definitive and intimate desires to the matchmakers at Tinder will open passion on demand, then more than a few are going to be tempted. And, while no one wants to sit in front of a recruiter and answer the question *Why do you want this job?* with unvarnished truth, if the information is transmitted to LinkedIn, which is empowered by data and algorithms to industriously deliver tantalizing professional opportunities from around the globe, then maybe the gain compensates the exposure.

How much will busy parents pay – in terms of revealed personal information – to find a vacation that brings their family together? How much raw biological data will patients transmit to healthcare enterprises – perhaps via an implanted microchip – for a guaranteed alert one hour before a heart attack? (Raghupathi & Raghupathi 2014) If the answer is everything, the codes and charts of our bodies, the full array of our memories, the whole psychological truth of our wanting, then we're leaning into personal transparency. It is an alarming prospect, but also a reasonable decision.

Transparency and authenticity

Transparency's first effect is integration of our selves: no aspect of our identity can be safely compartmentalized for selective distribution. Several years ago, news reports circulated of a woman living nocturnally as a sex worker while maintaining an ordinary daytime identity with an academic email address and typical social media postings. The two worlds kept their distance, until she and her clients began appearing in each other's "People You May Know" recommendations on Facebook. (Hill 2017) She tried to turn off the connections with the expected results, and so learned first-hand this rule of contemporary AI reality: normal schizophrenia – our almost theatrical ability to incarnate different selves in distinct times and contexts (Goffman 1959) – is jeopardized by the big

data invasion of privacy. Because being entirely known means being entirely known, the work-life and private-life distinction collapses into an encompassing identity. And there's no reason for confidence that the other aspects of our selves won't follow. As Facebook's Mark Zuckerberg perceived, "The days of you having a different image for your co-workers, and for the other people you know, are coming to an end (Kirkpatrick, 2011: 199).

The second transparency effect is fulfilled authenticity. As described within the Kierkegaard to Heidegger tradition, being who we are starts with the challenge of perceiving our own projects and endeavors amidst the distractions of others, and the busyness of quotidian life. Then there's the challenge of being resolute (Heidegger 1962: 354), of actively being true to that conception. Both these existential challenges recede, however, as personal transparency advances. We are not just exposed as who we are but, as the Facebook example underlines, we are increasingly *forced* to see and to be that person. The authenticity that used to be an achievement is threatening to become an affliction.

In small ways that, I submit, are not in the least trivial, this confinement by our own identity grows palpable as artificial intelligence gathers power. Taking Netflix as a common experience, it intersects users' personal information with predictive analytics to begin rolling the next film before the previous ends, meaning you get what you want before making any choices at all. On one level, you don't select another movie from a list and, above that, you don't even decide whether to watch another movie as opposed to reading or something else because it's already going. It's a trap. A pleasurable trap, but knowing that doesn't change the fact that it's hard to escape a viewing experience that reflects exactly what you like, and who you are as a video consumer.

One video autoplayed for me showed a restaurant operating with a near complete personal data set for each patron (Hang the DJ, 2017). The critical scene depicts a couple being served their dishes with perfect anticipation, just as they are about to ask for menus. More than a display of hyper-efficiency, the service

illustrates what pure consumer satisfaction means within the context of the AI human condition. If the food arrives *before* hunger (or if the next video starts before the previous finishes), then dissatisfaction rises because the food gets cold or the previous video gets interrupted. But, if the service is delivered *after* the urge for it, discomfort enters again as the sharp feeling of unanswered wanting. Now, in between these two dissatisfactions there is predictive analytics timing: you get what you want as the urge initiates, and to the degree required to stifle the wanting. There is, in other words, a critical moment. It is experienced when a desire is answered so immediately that you don't have time to understand *why* the response is right, when you started wanting it, or even to ask what it is that you wanted in the first place.

A curiosity about life as fully exposed and accurately served is that the way to realize something is what we want is: we *already* have it. And that's the only way we know we want something. More, if we do feel an urge to binge Seinfeld or taste a pizza slice, what that really means is: we don't actually want it. We can't since the whole idea of predictive analytics functioning with full access to our personal information is that the economic mechanisms know us transparently, and so respond to us by not allowing even an instant of unfulfillment.

If we had more time, we could ask whether something truly satisfies if we get it before hungering for it, or whether it feels good to *always* feel good. Regardless, the drowning of personal desire in convenience and delight is not a criticism of surveillance capitalism, it's a temptation. And one that implies a counter-intuitive exchange. We get personal authenticity as a life of satisfactions incarnating who we are. It's also true though, that we have no personal freedom to determine who that someone is. Since there's no experimenting with new possibilities, or struggling with what's worth pursuing, there's no room for creating an identity. We can only be who we already are, and so receive the bliss that recommended we fully expose ourselves to big data and predictive analytics in the first place. Personal transparency means a life so authentic that we can't do anything with it.

Personal freedom and big data with predictive analytics

Against confining authenticity, there is ethics oriented toward freedom. Within the context of surveillance capitalism, achieving it implies short-circuiting predictive analytics and that, in turn, entails reducing the exposure of our personal information. There are three broad reduction strategies. One conceals the information, with examples including the legislative GDPR and the engineering of privacy-by-design (Jandl 2019). Another obfuscates, which is the strategy of confusing true data in a torrent of false information (Brunton & Nissenbaum 2016). The third possibility is explored in this essay, it is speculative and pressed to the extreme as a way of sharply developing the freedom side of the AI human condition.

The strategy is to become someone else, to develop new traits replacing the personal information that has been gathered to contain our identities. Individuals that can significantly shift who they are – change their habits, tastes, aspirations, wants, fears, values – gain immunity from the satisfying powers of predictive analytics because the pleasures offered no longer apply to the person they target. In the Netflix example, I'm no longer trapped by the screen if the programs channeled to begin automatically are not tailored to the person I have become. Like anyone else, I stop watching when I'm not enjoying what I'm seeing.

Identity transformations sufficiently powerful to crack big data profiles are common, if not frequent. People recreate who they are seismically when they go away to college, marry, have children. Think of the kinds of things people choose for their screens (or, do and want around 3 a.m.) at each of those stages. The stark differences measure how badly the connections and incentives aimed by social media platforms and marketers suddenly begin to miss as individuals cross significant life thresholds (Kevina and Lawlor 2011). It's not just that the predictions are off-target, it's that they cannot possibly be on target because they aim for people who are no longer there.

There are also more surreptitious opportunities for immunity from our own pasts, some hiding underneath the very platforms and technologies that threaten to build inescapable identity data banks. Take LinkedIn. Designed to harvest personal information and then display job openings curated for information-modelled users (Staddon 2009), the platform doesn't just offer, it also excludes, it methodically eliminates opportunities falling outside data-established lines. So, nurses receive leads for new posts at other hospitals and in elder care businesses and, just as industriously, get shielded from openings in accounting departments and at law firms. With a little search ingenuity, though, users can discover options their own past information would otherwise prohibit (Hathuc 2016). By plugging in some misinformation about himself, the Silicon Valley entrepreneur may get matched to a corporate post in the Swedish welfare state. Or, a feminist can rewrite her biography, purchase a headscarf, and end up with a one-way ticket to an English-teaching job in Saudi Arabia. More life jarring opportunities are out there. Simply inputting imaginative educational degrees, for example, twists LinkedIn's algorithms to produces deviant job recommendations (Dinesh and Radhika 2014). And for those who transmit a resonant appeal to the recruiter who's willing to take a chance, they can be gone the next day.

Platforms designed to generate music playlists can be detoured, romantic matchmaking applications can be perverted (Stoyanova 2015). The list of possibilities for generating encounters entirely detached from established habits and tastes goes on nearly as long as the app store catalog. So while it's true that it has never been harder to not be who we are because the identity we've compiled digitally keeps tagging along behind us, it has also never been easier to get out of who we are, to disrupt our existences from the bottom up by connecting with unfamiliar urges and potentials. When that happens, lives regenerate with virgin data, personal information that hasn't been scraped and commodified for the surveillance marketplace.

Freedom and inauthenticity

The scraping and commodification will come again, though, because big data economic reality means the information merchants will always be catching up. People can establish unforeseen privacy zones, but the data gatherers can also keep searching phone locations and tracking credit card histories and scanning faces and monitoring social media accounts and resolving, inexorably, their personal information profiles (Gartner, 2016).

To stay ahead of the surveillance capitalists, what's needed is not just identity generation, but regeneration in the excessive sense Georges Bataille describes (Bataille 1991): the work of becoming other needs to impel its own repetition. Inauthenticity, that means, becomes a guiding virtue. Since the endeavor is to escape accumulated personal information by reassembling it differently and constantly, the only possible reason for consolidating a sense of self at any time and place is *in order* to become someone else. Valorized inauthenticity lets that happen. By debasing loyalty to the idea of genuine I, it opens the way to identity's transformation from termination to station in the sense that arrivals only come to leave.

Where the Heideggerian organizes human experience around self-understanding that endures despite of the world's haphazard occurrences and distractions, the intentionally inauthentic embrace the arbitrary as opportunity. For example, a job announcement discovered by chance and explored on a whim may be irreconcilable with posts previously held, may deviate from a career path, may demand relocation to a foreign place geographically or psychologically. It may, in other words, be inauthentic in this sense: by converting the marginal into the essential, it forgoes responsibility for longstanding projects, and for all those others who have been incorporated into them.

The work of inauthenticity also leverages abruptness. Existentially, this is the impulse to buy a one-way airline ticket, or the frivolous engagement with a romantic partner who shares few interests, common experiences or mutual friends.

As an enabling attitude, inauthenticity converts superficiality, spontaneity and impulsiveness from character defects into powers.

From inauthentic existence, a narrow human freedom emerges. More exploratory than selective, personal autonomy in the time of big data is not about choosing from known options so much as deciding between the collection of familiar possibilities, and the unknown. When the entrepreneur goes corporate, or the feminist goes to Arabia, these aren't weighed opportunities selected from a menu of predictable futures, they are blind leaps. And since the entire point is to recreate the self in unforeseeable ways escaping the information previously gathered to capture who we are, it's an odd sort of freedom because it aims to be impossible – and to make it impossible – to locate the person who experiences it.

The AI human condition

Ethics from Kierkegaard to Heidegger conceived authenticity as entwined with freedom and its expression. Ethics in the AI human condition is a dilemma between total exposure and recreative identities: either authenticity without freedom or freedom without authenticity.

References

Bataille, Georges, 1991, *The Accursed Share*, New York: Zone Books.

Brunton, Finn and Nissenbaum, Helen, 2016, *Obfuscation: A User's Guide for Privacy and Protest*, Boston: MIT Press.

Colley, Linda, 2000, "Going Native, Telling Tales: Captivity, Collaborations and Empire," *Past and Present,* 168: 170-193.

Connolly, Byron, 2014, Don't cross the 'creepy line' of dataanalytics, *CIO Australia*, http://www.cio.com.au/article/538947/don_t_cross_creepy_line_data_analytics/ Accessed 2 February 2020.

Dinesh, Kumar. and Radhika, V., 2014, A Survey on Predicting Student Performance, *International Journal of Computer Science and Information Technologies*, 5(5):6147–9.

Deleuze, Gilles, 1983, Plato and the Simulacrum, *October.* 27: Winter, Cambridge: MIT Press.

Gartner, 2016, How to Choose a Data Broker. https://www.gartner.com/smarterwithgartner/how-to-choose-a-data-broker. Accessed 11 January 2020.

Goffman, Erving, 1959, *The Presentation of Self in Everyday Life*, New York : Anchor Books.

Guignon, Charles, 2004, *On Being Authentic*, London: Routledge.

Hang the DJ, 2017, *Black Mirror*, Writer Charlie Brooker, Director Tim Van, Netflix.

Hathuc, Viet; Xu, Ye; Pradeep, Satya; Kanduri, Wu, Xianren; Dialani, Vijay; Gupta, Abhishek; Sinha, Shakti, 2016, Search by Ideal Candidates: Next Generation of Talent Search at LinkedIn, *Proceedings of the 25th International Conference Companion on World Wide Web (WWW '16 Companion)*, International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, CHE, 195–198. DOI:10.1145/2872518.2890549.

Heidegger, Martin, 1962, *Being and Time*, trans Macquarrie and Robinson. Oxford: Basil Blackwell.

Hill, Kashmir, 2017, *How Facebook Outs Sex Workers*, Gizmodo. https://gizmodo.com/howfacebook-outs-sex-workers-1818861596. Accessed 24 January 2020.

Jandl, Christian; Nurgazina, Jamilya; Schöffer, Lucas; Reichl, Christian; Wagner, Markus; Moser, Thomas, 2019, SensiTrack - A Privacy by Design Concept for Industrial IoT Applications, 24th IEEE International Conference on Emerging Technologies and Factory Automation, 10-13 September. 2019. DOI: 10.1109/ETFA.2019.8869186.

Kevina, Cody and Lawlor, Katrina, 2011, On the Borderline: Exploring Liminal Consumption and the Negotiation of Threshold Selves, *Marketing Theory* 11, no. 2: 207–28. DOI:10.1177/1470593111403220.

Kirkpatrick, David, 2011, *The Facebook Effect*, New York: Simon & Schuster.

Menke, Christoph, 2005, "Innere Natur und Soziale Normativität: Die Idee der Selbstverwirklichung", in *Die kulturellen Werte Europas*, edited by Hans Joas and Klaus Wiegandt, Frankfurt am Main: Fischer, pp. 304–352.

Raghupathi, Wullianallur and Raghupathi, Viju, 2014, Big Data Analytics in Healthcare: Promise and Potential. *Health Information Science and Systems*, 2:3. DOI: 10.1186/2047-2501-2-3.

Sprenger, Polly, 1999, Sun on Privacy: Get Over It. *Wired*. January 26, 1999. Accessed March 24, 2018: https://www.wired.com/1999/01/sun-on-privacy-get-over-it/

Staddon, Jessica, 2009, Finding "Hidden" Connections on LinkedIn An Argument for More Pragmatic Social Network Privacy, *Proceedings of the 2nd ACM Workshop on Security and Artificial Intelligence (AISec 2009)*, ACM, New York, NY: 11-14. DOI: http://dx.doi.org/10.1145/1654988.1654992.

Stoyanova, Minka, 2015, Gaming Systems: Creative Critiques of the Ludic Real, *Datafied Research*, Vol 4 No 1. DOI: 10.7146/aprja.v4i1.116105.

Takalkar, Madhumita, Xu, Min, Wu, Qiang, 2018, A Survey: Facial Micro-Expression Recognition, *Multimedia Tools and Applications*, 77: 19301. DOI: 10.1007/s11042-017-5317-2.

Voas, Jeffery and Kshetri, Nir, 2017, Human Tagging, *Computer*, 50:10. DOI: 10.1109/MC.2017.3641646.

Zuboff, Shoshana, 2015, Big other: surveillance capitalism and the prospects of an information civilization, *Journal of Information Technology*, 30:1, pp 75–89. DOI: 10.1057/jit.2015.5.

Zuboff, Shoshana, 2019, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York: Hatchette.

END