

Fair trade: Your soul for data?

November 12 2019, by Dr Retha Langa



Credit: CC0 Public Domain

In an increasingly data-driven world, are we just walking data sources for the benefit of giant multinational corporations?

Every single minute, there are 3.8 million search queries on Google; 4.5 million videos watched on YouTube; almost \$1 million spent online; 41.6 million messages sent via WhatsApp and Facebook

Messenger—and these are a fraction of the interactions that currently happen online.

As we go about our daily lives—sharing our [personal experiences](#) on social media, asking Siri to set our alarms, and counting how many steps we walk on our wearables—we are essentially becoming walking data points, where our information is collected and analysed to predict behaviour. Where will it end?

Professor Turgay Celik, Director of the National e-Science Postgraduate Teaching and Training Platform (NEPTTP) and the Wits Institute of Data Science (WIDS), predicts that in the next 10 to 15 years, humans will be "directly connected to cyber space without using devices. [Your brain will be directly connected to the internet](#)," he says.

Wits Biomedical engineers have already connected a human brain to the internet in real time. This Brainternet project essentially turned the brain into an Internet of Things node on the World Wide Web.

In 2019, the same team connected two computers through the human brain and transmitted words like 'hello' and 'apple', passively, without the user being aware that a message was present.

"Do we really need to have our physical bodies to experience life, or do we only need to have our own brain?" asks Celik. "We will be seeing the systems creating those virtual environments to give humans an experience of nature. You want to go and see the ocean, but do you really need to physically go there? Can I stimulate a part of my brain to give me that experience?"

Android rights and the Big Other

Dr. Christopher Wareham, Senior Lecturer in the Steve Biko Centre for

Bioethics at Wits argues that we need to think about the implications of such technological developments from the perspective of artificial agents. These "digital beings" will potentially have lives—and rights—of their own.

"Traditionally the focus on this question is very much on the other side of the issue: How are we going to stop them from harming us? There is very little work that looks at it from the other side. How are we going to prevent humans from harming this being, experimenting on it? Should there be laws that protect this type of being?"

The developments in machine learning and artificial intelligence (AI) already significantly affect how we live our lives today. American academic Shoshana Zuboff coined the term 'surveillance capitalism' in 2014. Surveillance capitalism depends on "the global architecture of computer mediation... [which] produces a distributed and largely uncontested new expression of power". Zuboff christens this the "Big Other". Currently, the "Big Other" includes Facebook, Google, Microsoft and Amazon.

Surveillance capitalism

Writing in *The Guardian*, Zuboff explains, "The logic of surveillance capitalism begins with unilaterally claiming the private human experience as free raw material for production and sales. These experiences are translated into behavioural data. Some of this data may be applied to product or service improvements, and the rest is valued for its predictive power. These flows of predictive data are fed into computational products that predict human behaviour."

Surveillance capitalism is a "real issue", says Professor Brian Armstrong, Chair in Digital Business at the Wits Business School. "In my view, a very big concern is around the whole idea of social scoring." This refers

to the practice of developing a social rating system to establish if a person is a fit and proper member of society, in terms of their "social score".

In China, [private companies](#) are already operating social credit systems, as is local government in pilot projects. The plan is to develop a nationwide system that scores the individual's behaviour, including giving citizens a score and adding rewards and penalties for specific actions. For example, if you donate to charity, you score points but you lose points for traffic violations.

But one need not look as far as China for Big Brother-style surveillance. In Johannesburg, thousands of surveillance cameras already monitor motorists and pedestrians 24/7. In June, the Financial Mail reported that Vumacam—a subsidiary of internet fibre company, Vumatel—had installed more than 1,200 surveillance cameras to combat crime. By 2020, the number of cameras will increase to over 10,000.

Local security companies can access the Vumacam live feed and, as the artificial intelligence system learns what a typical day in a neighbourhood looks like, it will flag behaviour that is out of the ordinary for that area. Dr. Helen Robertson, who lectures Data Privacy and Ethics in the School of Computer Science and Applied Mathematics, refers to the battle between our right to safety and our right to privacy that such forms of surveillance bring to the fore.

"It strikes me as plausible that we think our claims to safety have increased weight in contrast with our claims to privacy. If the relevant algorithms are going to identify abnormalities in the footage, we need to keep in mind how good these algorithms are or aren't."

Safety vs. privacy

Our views on privacy have not only been impacted by safety concerns. The pervasiveness of [social media](#) has also played a role. Robertson says that the average person is willing to share a lot more about their private lives today compared to a few decades ago. These evolving views are not necessarily problematic. "It might simply be a matter of one society's convention in contrast with another society's convention, and how they tend to feel with regard to how much they are willing to share."

Celik believes that privacy will become personalised, with individuals being able to define how much privacy they want for themselves.

Our autonomy is another area influenced by the online world. Wareham argues that a lot of micro-targeted advertising and political messaging is designed specifically to degrade our autonomy. "If you do a Google search now, you're not going to get an unbiased sample of information ... you're going to get information that Google has catered for you to get ... these sorts of micro-targeting ... want to trigger you through nudges to behave in certain non-rational ways."

The question then becomes about who decides what you read, listen to, or watch, and who makes the decisions on what content is "appropriate" for a specific digital platform, and what is not.

Toward tech that teaches

Data-driven advancements are, however, not all doom and gloom. "Data in itself is not agnostically good or bad, but it is what we do with it. It can be abused, or it can be used for very positive purposes," argues Armstrong, adding that education is one area in which South Africa could benefit immensely.

"If we were able to use learning management systems more efficiently to see how students are learning, to see what material they are struggling

with ... to learn what teaching styles work best, we can individualise the learning experience."

In China, AI-enabled education has already blossomed with tens of millions of students using some form of AI to learn. This includes tutoring platforms where algorithms curate lessons and adapt the curriculum based on an individual's understanding of specific concepts, reports MIT Technology Review.

Protecting personal data

Staggering amounts of data are generated daily, but who owns all this data? Robertson points out that there is currently no consensus among ethicists about this thorny issue.

Some argue that the data subject owns the data. Others say that the data processor who uses his/her resources to create and analyse a dataset has ownership rights, while some argue that in certain cases, such as medical research that benefits society, the public's need for medical treatment and breakthroughs mean that data belong to the public.

These different claims to ownership "add a lot of ethical greyness", says Robertson. "The ownership of data is particularly difficult. It is an object that can be traded, but at the same time, it has a reference to an individual, something like other artefacts do, such as photographs. The rights certainly seem to pull in different directions."

In the near future, South Africans will have considerable legal power regarding the protection of their data. The Protection of Personal Information Act (POPIA) aims to protect the right to privacy, while enabling the social and economic benefits that result from the free flow of information. POPIA stipulates conditions under which personal information must be processed lawfully, although there are exceptions.

These conditions include that personal information "must be collected for a specific, explicitly defined and lawful purpose". Further processing of personal information can only take place if it is in line with the purpose for which it was originally collected. Most sections of the Act have not yet commenced. The announcement of a commencement date is expected before the end of 2019, after which companies will have one year to comply.

Verine Etsebeth, a Senior Lecturer in the Wits School of Law who specialises in data protection and information security law, says the POPI Act is long overdue. "The sooner it is in practice, the sooner it can come before our courts and we can have precedents set," says Etsebeth. "It is going to be survival of the fittest. If your competitor complies and you don't, you won't be able to retain your customers. Companies will realise just how much their reputations are worth."

Digital disempowerment

Despite the excitement over technology's potential to solve some of our most complex problems, many South Africans are still excluded from these advances. Only 40% of Africa's population has access to the internet compared to 61% for the rest of the world. In South Africa, internet penetration currently sits at 56%.

"In today's world, digital disempowerment is one of the most profound forms of disempowerment," says Armstrong. "Digital disempowerment comes in three levels. The first is do you have access, secondly do you use it, and thirdly are you engaged, transacting and impacted? In South Africa, you don't have access if the networks don't cover where you are, or if you can't afford the mobile device ... or if you can't afford the price of data. In all of those areas we have a challenge."

Provided by Wits University

Citation: Fair trade: Your soul for data? (2019, November 12) retrieved 23 April 2024 from <https://techxplore.com/news/2019-11-fair-soul.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.