centric.org.uk

FROM "DON'T BE EVIL" TO "CAN'T BE EVIL" - A PARADIGM SHIFT FOR AI & DATA PRIVACY

By Yunus Skeete

Software Engineer, Privacy-Preserving AI

centric.org.uk

AI arguably presents the biggest opportunity for advancement in human history:

“I’ve always thought of AI as the most profound technology humanity is working on - more profound than fire or electricity or anything that we’ve done in the past,” commented Google CEO, Sundar Pichai, on the current developments in Artificial Intelligence (AI) [1].

“We are developing technology which, for sure, one day will be far more capable than anything we’ve ever seen before.”

“More profound than fire or electricity...”

“Well, it kills people, too,” Pichai noted about the perils of fire in 2018 [2]. “We have learned to harness fire for the benefits of humanity, but we had to overcome its downsides, too,” Pichai continued, comparing the task at hand in managing the threats of AI to those humanity previously overcame with fire. In another interview, Pichai questioned: “How do you develop AI systems that are aligned to human values - and including - morality?” [3].

This article does not address questions about how to ensure that the sentient AI of the future is moral. Rather, we focus on a more pressing issue about the emerging AI of today: ***in an AI world set to capture and monetise your personal data, how do we develop AI systems that are aligned to another central human value - privacy?***

The potential for a country to monetise its advancements in AI is causing a blind chase for technological progression:

“Whoever leads in artificial intelligence by 2030 will rule the world until 2100.” [4]

The stakes could hardly be higher; seldom do epochal opportunities arise for countries to put themselves at the forefront of the global economy through the goods and services that they produce. The trick is to get there first.
With its ability to impact every other industry on the planet, AI is the biggest opportunity to date. Naturally, then, there is plenty of domestic incentive for AI innovation and commercialisation.

AI contributed £3.7 billion to the UK economy last year alone. By 2030, UK GDP promises to be 10.3% higher as a result of artificial intelligence [5].
In other words, by the end of the decade, AI’s contribution to the UK economy will match that of all domestic trade (as of Q4 2022) [6]. Such is the scale of this occasion that technology policy may effectively become the new economic policy. The UK has acknowledged this with a £1 billion AI grant to establish the UK as a science and technology superpower [7].

An area at the forefront of AI that the UK is positioned competitively in is the emerging field of autonomous vehicles: The first autonomous bus in the UK launched in Scotland earlier this year [8]; Asda have partnered with London-based Wayve to launch UK’s largest self-driving grocery delivery trial [9];
The UK government has proposed new laws facilitating a rollout of self-driving vehicles by 2025 whilst its £100m in state funding seeks to catalyse the autonomous vehicle industry.

The plans for the ubiquitous adoption of large-scale and pervasive AI within autonomous vehicles are already well in motion. What risks do such advancements pose to our privacy, however?

Facilitating these advancements are larger, more pervasive AI models, trained on ever-more of our (private) data, giving hitherto unforeseen levels of insight and power to corporate entities:

Individual data privacy - or the ability to control who is told what about us, and when - is of utmost importance when concerning where we are, where we're going and where we live.

The estimated 2,600,000 cars in London make automobiles distinctly more prevalent than the estimated 942,562 CCTV cameras in the UK's Capital [10]. Of note, however, is that the nature of our potential exposure to autonomous vehicles is starkly different to CCTV cameras, which, although operating in far less private and residential settings, capture us up to 70 times per day on average [11].

CCTV exposure as it currently stands would already be able to paint a fairly good picture of where we are, where we're going and where we live, if not for strict legislative protection not yet afforded to emerging autonomous vehicles. Scaling up this exposure as self-driving cars promises to do, and continuing to omit similar levels of regulatory constraints, grants corporate entities insight (and therefore power) on an unprecedented scale. Ensuring British citizens retain control over their privacy must be of primary concern as without sufficient protective measures, the future of autonomy may foreshadow the future of surveillance.

'Large-scale, mobile, pervasive, privately-owned and underregulated video and audio surveillance systems' - this is the most pessimistic forecast of the future of autonomous vehicles. The likelihood of this threat materialising hinges on whether industry abuses the unprecedented levels of insight and power that technology and government policy affords corporate entities. So how well have they been managing it thus far?

With recent data privacy breaches in autonomous vehicles, developments in autonomous vehicle AI threaten to put the UK public at unprecedented levels of risk:

To develop its self-driving car technology, the popular electric vehicle manufacturer, Tesla, collects vast amounts of data from its global fleet of several million vehicles. Caught up in a recent data-privacy controversy, former Tesla employees were quoted with the following:

“Tesla would receive video recordings from its vehicles even when they were off.” According to nine former employees, the “scandalous” videos - including one of a customer approaching a car completely naked - were collected without consumer awareness and shared by Tesla employees in an internal messaging system: **“Any normal human being would be appalled by this...”**

“We could see inside people’s garages and their private properties,” employees reported. “We could see them doing laundry and really intimate things. We could see their kids.” Commenting on Tesla’s ability to view the location of recordings on Google Maps, one employee labelled the fiasco as a “massive invasion of privacy” [12].

The response to this controversy has been strong: “Any normal human being would be appalled by this,” David Choffnes of the Cybersecurity and Privacy Institute at Northeastern University commented, labelling the scandal as “morally reprehensible.” In China, some government compounds and residential neighbourhoods have banned Tesla cars due to concerns about their cameras. Addressing the issue in a virtual talk at a Chinese forum in 2021, Tesla CEO Elon Musk said: “If Tesla used cars to spy in China or anywhere, we will get shut down.”

Closer to home, the shutting-down of ill-regulated tech products is how some municipalities have sought to protect their citizens...

The social contract governing this technology is a “don’t be evil” plea to industry, which, in light of recent high-profile scandals, is proving inept at protecting public privacy:

Regulators in the West have expressed concern about laws that allow the Chinese government to secretly demand data from Chinese companies and citizens for “intelligence-gathering operations”.

Recently, the USA and Canada have joined a growing list of EU countries seeking to ban TikTok - a product of the Chinese company BtyeDance - due to fears of mass surveillance by the Chinese government [13]. These sentiments have only intensified in light of recent news in which TikTok admitted to tracking a British journalist, to try to establish who was secretly meeting with the press, through a TikTok account she created for her cat [14].

TikTok, however, isn’t a nation-wide fleet of pervasive, mobile, location-aware, AI-powered and controllable audiovisual surveillance systems. With the doors for services like TikTok currently still open to Chinese multinationals, access to the UK markets for autonomous vehicles still remains under lock and key, right? Wrong.

With China a forerunner in self-driving car innovation, and contributing just under a third of global vehicle production, it would seem a matter of time before Chinese autonomous vehicles enter UK markets [15]. A fleet of autonomous vehicles under overbearing foreign jurisdiction then rapidly begins to resemble our worst surveillance nightmares.

In a global race to dominate and export AI goods and services, overbearing regulatory pressures are out of the question - if regulators could even keep up with the pace of innovation, that is. Hence, without infrastructure obeying a “privacy-preservation by design” philosophy, we are collectively making the biggest corporate plea of “don’t be evil” in human history. Current AI innovation gives the keys to a back door - that has never left us more exposed - to anyone who asks. The question begs: how comfortable are we with this? And what is to be done about it?

(CONCLUSION)

A paradigm shift for AI and data privacy - from "don't be evil" to "can't be evil" - is needed to protect public interests:

Tighter regulation would mandate stronger privacy guarantees for the individual. With governments financially dis-incentivised to curtail AI developments, however, the drive for privacy-preserving AI must come from elsewhere.

This paradigm shift is currently being facilitated by the emerging fields of privacy-enhancing technologies and privacy-preserving artificial intelligence. Such promises to make privacy violations like the aforementioned impossible.

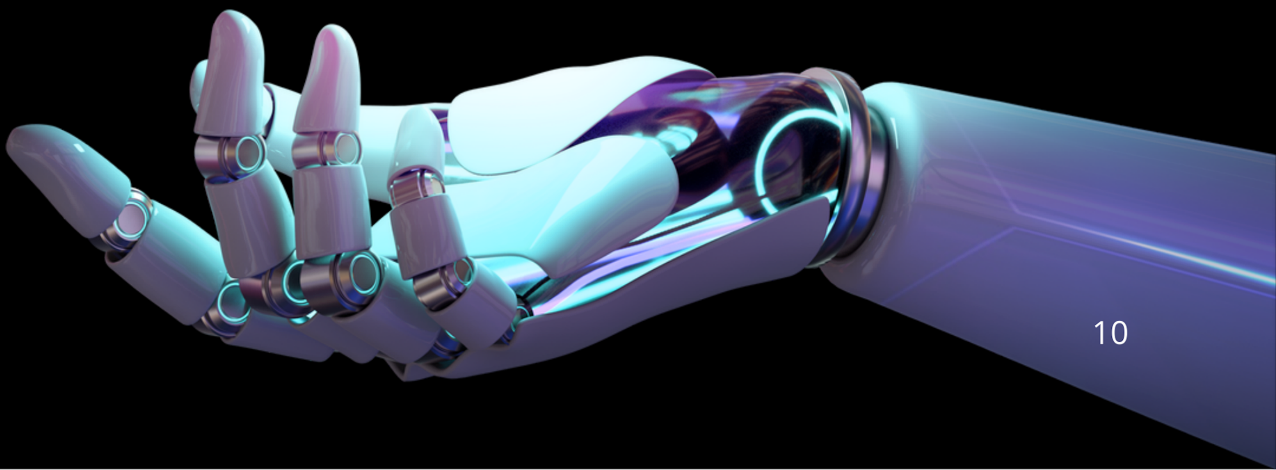
Within the field of autonomous vehicles, companies like Wayve are relying heavily on simulation and synthetic data generation. This minimises the need to train their algorithms on vehicles streaming video to AI engineers as they drive down your street. However, once these fully-trained and production-ready AI systems take to the streets, many questions need to be answered about how such operations will mitigate the privacy risk posed to the public. Much progress is needed within the industry to implement privacy-enhancing technologies which make the shift from "don't be evil" to "can't be evil".

Elsewhere, in the medical industry, the Melloddy project brings together a group of pharmacological research entities for drug discovery. Built upon their privacy-preserving AI platform, Substra, Melloddy ensures that sensitive corporate data can be put to good use by AI, without leaking any unwanted information.

This is facilitating unprecedented levels of commercial collaboration, driving the industry forward. Owkin, the parent company, is working to bring privacy-preserving AI to healthcare patients like you and I. They are doing this by applying privacy-enhancing technologies and AI to sensitive patient data and medical records such that AI can extract all of the implicit value from it without the data ever needing to be shared.

Well-defined “privacy-by-design” data pipelines and AI systems will allow us to have our AI cake and eat it too - no longer will the public need to fear for their privacy. If AI is to be more profound than fire or electricity, it will need to pass all of society’s social acceptability tests. In the long-term, socially-harmonious AI is the only AI that will endure.

It is less likely to be whoever leads in artificial intelligence by 2030 who will rule the world until 2100, but rather whoever leads in responsible and sustainable artificial intelligence. To endure, we must develop AI systems that are aligned to human values - namely privacy. Hence, states and corporate entities who seek to lead in the pervasive AI of the future will need to be foremost proponents of a paradigm shift for AI and Data Privacy from “don’t be evil” to “can’t be evil.”



Bibliography

1. Prakash, P. (2023) Alphabet CEO Sundar Pichai says that A.I. could be ‘more profound’ than both fire and electricity-but he’s been saying the same thing for years, Fortune. Available at: https://fortune.com/2023/04/17/sundar-pichai-a-i-more-profound-than-fire-electricity/ (Accessed: 22 May 2023).

2. Clifford, C. (2018) Google CEO: A.I. is more important than fire or electricity, CNBC. Available at: https://www.cnbc.com/2018/02/01/google-ceo-sundar-pichai-ai-is-more-important-than-fire-electricity.html (Accessed: 22 May 2023).

3. Pelley, S. (2023) Is artificial intelligence advancing too quickly? what AI leaders at Google say, CBS News. Available at: https://www.cbsnews.com/news/google-artificial-intelligence-future-60-minutes-transcript-2023-04-16/ (Accessed: 22 May 2023).

4. Gill, I. (2020) Whoever leads in artificial intelligence in 2030 will rule the world until 2100, Brookings. Available at: https://www.brookings.edu/blog/future-development/2020/01/17/whoever-leads-in-artificial-intelligence-in-2030 -will-rule-the-world-until-2100/ (Accessed: 22 May 2023).

5. PwC (2017) The economic impact of artificial intelligence on the UK economy - PWC UK, PwC. Available at: https://www.pwc.co.uk/economic-services/assets/ai-uk-report-v2.pdf (Accessed: 22 May 2023).

6. McCrae, R. (2023) Balance of payments, UK: October to December 2022, Balance of payments, UK - Office for National Statistics. Available at: https://www.ons.gov.uk/economy/nationalaccounts/balanceofpayments/bulletins/balanceofpayments/octoberto december2022 (Accessed: 22 May 2023).

7. Donelan, M. (2023) Government commits up to £3.5 billion to future of tech and science, GOV.UK. Available at: https://www.gov.uk/government/news/government-commits-up-to-35-billion-to-future-of-tech-and-science (Accessed: 22 May 2023).

8. Shapps, G. (2023) UK government backing helps Launch World First Self-driving bus, GOV.UK. Available at: https://www.gov.uk/government/news/uk-government-backing-helps-launch-world-first-self-driving-bus (Accessed: 22 May 2023).

Bibliography

9. Wayve (2023) Asda and WAYVE launch UK's largest self-driving grocery home delivery trial, Wayve. Available at: https://wayve.ai/press/asda-and-wayve-launch-grocery-delivery-trial/ (Accessed: 22 May 2023).

10. TfL (2012) Technical note 12 - how many cars are there in London and who owns them?, Roads Task Force – Technical Note 12 How many cars are there in London and who owns them? Available at: https://content.tfl.gov.uk/technical-note-12-how-many-cars-are-there-in-london.pdf (Accessed: 22 May 2023).

11. Barker, R. (2022) How many CCTV cameras in London? UK CCTV numbers (updated 2022), Clarion UK. Available at: https://clarionuk.com/resources/how-many-cctv-cameras-are-in-london/ (Accessed: 22 May 2023).

12. Mathers, M. (2023) Tesla Workers Shared Video of Naked Customer Taken On Vehicle Camera, The Independent. Available at: https://www.independent.co.uk/news/world/americas/tesla-workers-video-naked-customer-b2315922.html (Accessed: 22 May 2023).

13. Maheshwari, S. and Holpuch, A. (2023) Why countries are trying to ban TikTok, The New York Times. Available at: https://www.nytimes.com/article/tiktok-ban.html (Accessed: 22 May 2023).

14. Kleinman, Z. (2023) Tiktok tracked UK journalist via her cat's account, BBC News. Available at: https://www.bbc.co.uk/news/technology-65126056 (Accessed: 22 May 2023).

15. 灿崔 (2022) A look at strength of Chinese cities in auto industry, A look at strength of Chinese cities in auto industry- China.org.cn. Available at: http://www.china.org.cn/china/2022-08/15/content_78373080.htm (Accessed: 22 May 2023).

THANKYOU

CONTACT

welcome@centric.org.uk