GlobalResearch
Center for Research on Globalization

Worse than Facial Recognition – the Next Big Privacy Outrage

By True Publica
Global Research, October 14, 2019
TruePublica 13 October 2019

Region: Europe
Theme: Intelligence, Police State & Civil Rights

Privacy campaigners have warned of an "epidemic of facial recognition" use around the UK. This, of course, followed the epidemic of CCTV that led to it in the first place. An investigation by Big Brother Watch, the civil liberties campaign group, found major property developers, shopping centres, museums, conference centres and casinos were using the technology in the UK. The police use it – with startlingly high failure rates. But now comes a new battleground in the privacy war – lie detection systems.

At TruePublica, we have warned about the rise of the UK's techno-Stasi-state where technology is harnessed and used against the civilian population without any debate or indeed any real legal framework. But if you think that facial recognition is bad enough, then the next outrage against our civil liberties is already being rolled out – again, with no public debate. This time, civil society is being tested with AI-driven lie detection systems – and this is very much worse than facial recognition with more challenging implications.

There are literally hundreds of studies that have examined the 'Pinnochio Effect' of humans and a quick online search provides many answers. Generally speaking, it is understood that we all tell one or two big lies a day and a few 'white lies' – and are then exposed to hundreds from others collectively. Lies range from being socially polite to covert reasons for personal advancement or indeed, to actively harm others. But then, we all know that. That's why we trust some and not others. That's why some truly inadequate, useless people get good jobs and others don't. Lying is a game we all play, every day of our lives and we've learned to navigate it. Some better than others.

Technology has attempted to solve the problem of lying – or finding the truth, where a serious situation demands it. In cases of serious crimes, polygraphs would be great if they worked but they don't. And here's another lie. Invented in 1921, the Polygraph has put many behind bars in the USA. Some have been wrongfully put to death because of it. And yet, despite claims of 90% validity by polygraph advocates, the National Research Council has found no evidence of effectiveness and two-thirds of the scientific community who have the requisite background to evaluate polygraph procedures considered polygraphy to be little more than pseudoscience. And yet, there are about 2.5m polygraph exams still being conducted in the US every year in an industry worth $2.5 billion. It's not about getting to the truth, it's all about the money – as they say.

The UK has started using polygraphs which have been used on sex offenders since 2014, and in January 2019, the government announced plans to use it on domestic abusers on parole. So you might also be alarmed to know that a new wave of lie detection systems are not just on their way, they are already in use.

Many startups now claim that a powerful new generation of lie-detection tools are not just working but in active use. They want us to believe that a virtually infallible lie detector is, just like the polygraph was in the 1920s, just around the corner.

The consequence is that these new systems are being acquired by police forces and state agencies desperate to keep ahead of potential breaches of national security. Worse, they are also now being used by insurance companies, welfare officers and soon on the horizon – by employers. For example – the Converus website promotes a product called EyeDetect and makes claims of 90% accuracy just as polygraphs once did. Its homepage says –

> "EyeDetect® is a next-generation lie detector. It measures subtle changes in the eye to detect deception. EyeDetect is used to screen job applicants, employees, parolees, and immigrants — as well as law enforcement and public safety personnel — to protect against corruption and crime. It is also used to conduct diagnostic (single issue) testing for criminal or civil cases. When the truth matters, get a second opinion with EyeDetect."

In the meantime, the system is being used in the real world.

> "EyeDetect, has been used by FedEx in Panama and Uber in Mexico to screen out drivers with criminal histories, and by the credit ratings agency Experian, which tests its staff in Colombia to make sure they aren't manipulating the company's database to secure loans for family members. Other EyeDetect customers include the government of Afghanistan, McDonald's and dozens of local police departments in the US. Soon, large-scale lie-detection programmes could be coming to the borders of the US and the European Union, where they would flag potentially deceptive travellers for further questioning."

And before you know it that is exactly what then emerged.

The FT published a story last month on the subject –

> "A group of researchers are quietly commercialising an artificial intelligence-driven lie detector, which they hope will be the future of airport security. Discern Science International is the start-up behind a deception detection tool named the Avatar, which features a virtual border guard that asks travellers questions. The machine, which has been tested by border services and in airports, is designed to make the screening process at border security more efficient, and to weed out people with dangerous or illegal intentions more accurately than human guards are able to do."

Using technology is of course nothing new, what is new is that these systems require mass data to work in the first place. One system already trialled and in use uses AI to predict crime. The data looks at the number of crimes an individual had committed with the help of others and the number of crimes committed by people in that individual's social group. The result of tests showed there were serious ethical questions to answer and that the failure rate meant arresting innocent people.

Martin Innes, director of the Crime and Security Research Institute at Cardiff University, UK, says he is "sceptical" that the system will reliably predict offences at an individual level. The

tool will probably be more useful for generally locating communities at risk, he says.

Northumbria Police are carrying out a pilot scheme that uses EyeDetect to measure the rehabilitation of sex offenders. It won't be long before such systems are broadened to such an extent that using AI lie detection systems could be used on all matter of daily decision making.

In a recent Guardian article – "The race to create a perfect lie detector" – the author asks:

> "But as tools such as EyeDetect infiltrate more and more areas of public and private life, there are urgent questions to be answered about their scientific validity and ethical use. In our age of high surveillance and anxieties about all-powerful AIs, the idea that a machine could read our most personal thoughts feels more plausible than ever to us as individuals, and to the governments and corporations funding the new wave of lie-detection research. But what if states and employers come to believe in the power of a lie-detection technology that proves to be deeply biased – or that doesn't actually work?"

The bigger question to consider is if such technologies are indeed used what effect will that have on daily life for all of us? Human society is arranged by all sorts of different factors and being forced to tell the truth sounds OK if everyone does it, but those designing and controlling these systems may well be exempt as could law enforcement officers, and, even the politicians that authorise their use. Can you imagine advanced tools like these in the hands of populist leaders clinging onto power in a world full of fake news and post-truths to frame opponents or dissenters?

The other issue is that polygraphs have been used for convictions for decades. The first was in 1935 and hundreds of exonerations have since followed – and at the end of this long experiment, which has proven to be a failure its use is continued and worse, it's being rolled it out in the UK.

Lie detection is a completely new frontier and startups are targeting it in an age of national and domestic security, a way to combat the rising costs of policing the streets and then look at ways of making decisions about health (questionnaires about exercise, food, alcohol?), education (catchment areas?), employment (reasons for leaving last employer?) and all manner of normal life.

An increasing number of projects are using AI to combine multiple sources of evidence into a single measure for deception. Can you imagine a system that gives you deception rating? Machine learning is accelerating deception research by spotting previously unseen patterns in reams of data. The Guardian article highlights that Scientists at the University of Maryland, for example, have developed software that they claim can detect deception from courtroom footage with 88% accuracy.

> "The algorithms behind such tools are designed to improve continuously over time, and may ultimately end up basing their determinations of guilt and innocence on factors that even the humans who have programmed them don't understand. These tests are being trialled in job interviews, at border crossings and in police interviews, but as they become increasingly widespread, civil rights groups and scientists are growing more and more concerned about the dangers they could unleash on society."

Discern Science, is a software system, that boasts automated interviewing technology that aims to send a verdict to a human border guard within 45 seconds, who can either wave the traveller through or pull them aside for additional screening. These systems are already in use at Nogales in Arizona on the US-Mexico border, and with federal employees at Reagan Airport near Washington DC. Discern Science claims accuracy rates of between 83% and 85%. It hopes to sell them to airports, government institutions, mass transit hubs, and sports stadiums.

Trials were then conducted by Frontex, the EU border agency, which is now funding a competing system called iBorderCtrl, with its own virtual border guard. One aspect of iBorderCtrl is based on Silent Talker, a technology that has been in development at Manchester Metropolitan University since the early 2000s. Silent Talker uses an AI model to analyse more than 40 types of micro-gestures in the face and head; it only needs a camera and an internet connection to function. This system has a reported accuracy rate of 75% with the team that developed the AI algorithm going as far as to say that "We don't know how it works."

Back in July this year, London's Metropolitan Police's controversial trial of facial recognition technology to spot suspects failed to work 81% of the time, according to researchers. The researchers from the University of Essex said the problems were so bad that the use of facial recognition by the Met should be stopped immediately. And yet this system is still in operation and used by various police forces and private contractors.

The accuracy rates of 80-90% claimed by the likes of EyeDetect sound impressive, but applied at the scale of a border crossing, they would lead to thousands of innocent people being wrongly flagged for every genuine threat it identified. It might also mean that two out of every 10 terrorists easily slips through. One could say that conversely eight out ten don't – but the evidence for less sophisticated systems such as facial recognition tell us that that will not be the case.

This blind faith in new technologies such as lie detection is very worrying. The British state is already the worst offender of any democracy in the world today for illegal breaches of privacy data. The state has intruded to such as extent it knows who you are right now, where you live, who you slept with last night, where you went, who you met and has evidence of it all. It is now, without proper public debate rolling out biometric databases that will merge with health records and other state agencies such as HMRC, local authorities, the courts, schools and the like.

In May this year, the EU Council Presidency and European Parliament reached an informal agreement on the introduction of mandatory biometric national identity cards including a photo and two fingerprints. The rollout of this technology is now worldwide already, with Africa and India leading the charge. In some parts of the Middle East biometric cards are used for border control, accessing health, registering and taxing cars, paying fines and even utility bills.

The merging of all this data is a serious cyber-security threat to all of us and yet civil society seems to have no choice in the matter. We are all being dragged into a world with an all-seeing eye managed by the least trusted of institutions in society, that of the government and their agencies.

And as the claims of reliability increase, as they did with polygraphs, the more dangerous

they will become. And as the architecture of these systems is always pointed directly at the most vulnerable in society, the expectation is that unsafe convictions could rise and the data of innocents people inappropriately used.

The scandal over digital strip searches after serious sexual allegations made to police is a good example. Here police confiscate mobile phones from the victim and download its entire memory logs to determine some level of complicity. Big Brother Watch said –

> "These digital strip searches are not only cruel, invasive and causing major delays to investigations – they breach victims' fundamental rights and obstruct justice. These invasive practices are highly likely to infringe victims' data protection and privacy rights protected by the Data Protection Act and the Human Rights Act."

The next wave of suspects to follow the polygraphed dissidents of the 1950s and homosexuals in the 60s, the online searches for benefit claimants in the 2000s, and biometric analysis of asylum seekers and migrants today could just as easily be you and me next. Lie detection systems are a dreadful idea. The data collected, often wrong, like facial recognition images and polygraph results, could then added to national databases that make decisions over all manner of our lives and we would never know why things just seem to go against us. And who is to say that this information is not manipulated by the army of private contractors, public sector workers and government officials to target non-violent protestors – just as they do by reclassifying whistleblowers as foreign state spies. And then, of course, will come the mobile Apps wanting to cash in from the frailties and insecurities of humans. You can just imagine the destruction of personal relationships this will cause.

*

Note to readers: please click the share buttons above or below. Forward this article to your email lists. Crosspost on your blog site, internet forums. etc.

Featured image is from the author

The original source of this article is TruePublica
Copyright © True Publica, TruePublica, 2019

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: True Publica

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca