UK Government Goes Full Orwellian, Building Biometric Database On Every Single Citizen

When Theresa May became UK Prime Minister in 2016. She had once fought against the National Identity Card and national database program, but it has now reappeared in a worse form. TN Editor

We've been warning about this moment since the first day TruePublica went online. We said that the government would eventually take the biometric data of every single citizen living in Britain and use it for nefarious reasons. DNA, fingerprint, face, and even voice data will be included. But that's not all.

The excuse to be used, as ever, will be national security or terrorism, despite the huge fall in fatalities from terrorism and terror-related incidents since the 1970s.

Apart from crime-fighting, the Home Office also proposes in its long-awaited report that it will use the centralized database for vetting migrants on the streets and borders of Britain.

Not for the first time, civil rights groups argue that systems such as face recognition is faulty, dubiously legal, and collected without public consent. The outcry over Facebook, Cambridge Analytica and the EU referendum should, if nothing else, confirm that bulk data collection, used without either public debate or a legal basis is emphatically against our civil liberties.

However, the legality of the creation of a **centralised biometric database** will not stop a government who have been repeatedly caught breaking the law when it comes to privacy and data collection. Police, immigration, and passport agencies already collect DNA, face, and fingerprint data. On the latter, police forces across Britain now have fingerprint scanners on the streets of Britain with officers providing no more than a promise that fingerprint data taken will be erased if the person stopped is innocent of any crime.

The government's face database already has 12.5 million people – or so it has admitted to. The Home Office, embroiled in all sorts of privacy and surveillance legal cases caused a scandal last April when an official said it would simply be too expensive to remove innocent people from its criminal face databases of mugshots.

Without proper, enforcible regulation that can be fully scrutinised by civil society, there are many opportunities for the misuse of biometric data. It means nothing when the Home Office says its collection of biometric data will be "lawful," when it is found by the highest courts in both Britain and the EU of breaking basic surveillance and data protection laws. And what laws there are, remain deliberately ambiguous on how they will ethically collect, store, or share biometric data.

Without any obstacles put in its way, the Home Office has essentially granted itself the right to end anonymity of any type to all the people of Britain.

Big Brother Watch recently released a report detailing a staggering 90% false positive rate for its face recognition systems and then went on to describe the Home Office defence of these systems – "misleading, incompetent and authoritarian."

The fact that on Remembrance Sunday 2017, the Metropolitan Police used automated facial recognition to find so-called 'fixated individuals' – people not suspected of any crime, but who might be suffering mental health issues, should be a wake-up call for us all.

TruePublica has just reported on one local authority in Thurrock using databases and algorithms to deliver public services. More particularly it is surveilling its own systems and citizens to pinpoint and target certain families, vulnerable people, the homeless and anti-social behaviour. The system is called a "predictive modelling platform" and was only revealed through a freedom of information request by a local journalist.

Council data from housing, education, social care, benefits and debt all contribute to the creation of a profile that is used to predict whether a person is at risk or what services is provided. The profiles then assign people a score that indicates whether they need attention from social services. That risk score is stored in a centre where identifiable details are replaced with artificial ones, a process known as pseudonymised data.

The warning we gave was that it wouldn't be that long when all citizens will be given such scores by local councils, local authorities, the police and various other government agencies. The speed of implementation has surprised even us though. One should not forget that there are 78 high profile government agencies and a further 401 public bodies closely associated with them.

To be fair to Thurrock council the system has become so embedded within their social services system that it is responsible for 100 per cent of referrals to the Troubled Family programme, a government-led scheme aimed at early social work intervention. The council also claims it has an 80 per cent success rate in predicting children who are at risk and should enter safeguarding. It does not say how the system failed the

other 20 per cent or how it affected them.

However, there is a dark side to this. TruePublica warned two years ago that social scoring systems were on the way. We wrote in 2016 and then again in early 2017 as a result of an in-depth report by Civil Society Futures regarding a new wave of surveillance: *"Citizens are increasingly categorised and profiled according to data assemblages, for example through data scores or by social credit scores, as developed in China. The purpose of such scores is to predict future behaviour and allocate resources and eligibility for services (or punishment) accordingly. In other words, rules will be set for citizens to live by through data and algorithms."*

The government is now building, without debate such a system for all of its agencies to access and input. Once complete the next step will be to 'manage' population behaviour through social credit scores.

Current common forms of biometric data collection include – fingerprint templates, iris and retina templates, voiceprint, 2D or 3D facial structure map, hand and/or finger geometry map, vein recognition template, gait analysis map, blood DNA profiles, behavioural biometric profiles and others.

Read full story here…