GlobalResearch
Center for Research on Globalization

Britain: The Database State. Intrusive Surveillance

By True Publica
Global Research, May 23, 2019
TruePublica

Region: Europe
Theme: Intelligence

Britain is a surveillance state, the worst in the democratic West. In a short period of time, it has amassed a rather sordid history of citizen surveillance – and it continues to be unlawful. Last September's damning judgement of British security operations against its own people saw the European Court of Human Rights (ECHR) rule that the government had unlawfully obtained data from communications companies and didn't put in place safeguards around how it did it. But what does the state really know about us and what about the future?

Under **Theresa May** in the Home Office, the surveillance state became ever more paranoid. It became the most extreme surveillance architecture ever devised in the West – and still is. And it's getting worse.

They wanted it all – compromising (naked usually) images of you, your family and friends, what subscriptions you have, sexual orientation and preferences and with whom, earnings, expenditure and on what – places you visit, dates you went there, what you did when you were there.

The state is so out of control its own security services were diverted away from external threats towards us – law-abiding citizens. It was not long ago that MI5 and GCHQ were accused of infecting domestic civilian equipment with viruses so they could turn on TV's and mobile devices at will in people's homes, they recorded conversations and took photos, hacked into iOS, Apple systems and Android equipment, encryption was circumvented even when it was specifically outlawed. Britain's spy agencies worked with the American CIA and created more than 1,000 viruses and other types of malware to gain access to everyday items and either monitor or steal data. It is not known exactly how much information the state has gathered about its people.

Scale of Data

The police can now find out any information it wants from any government agency – and there are 25 of them and they collect from dozens of others. For instance, the Ministry for Justice (one of the 25) has thirty-three government agencies reporting to it. They include the courts and tribunals, prisons and probation, family justice and so on. There are another 20 non-ministerial departments, with yet more agencies. All collecting data, all the time.

Companies such as Experian collect electoral roll and tax information and then pass it on to the government. The scale of data collected by the state is unprecedented in human history.

The oldest known government database is the one that collects DNA. It is estimated that it has about 10 per cent of the population listed – many of whom have never been charged with anything ever. The government announced it had removed nearly 7 million individual

files – and then admitted it still has another 7 million. The second largest civilian police DNA database in the West is in Austria. That database holds just 1 per cent of its population.

In Britain, the law allows police to take DNA samples for offences as minor as begging or being drunk and even taking part in a demonstration or protest that was not pre-approved by them. They can demand fingerprints on the streets and access extremely private data without any permissions or real oversight and illegally amass facial recognition data at sporting events and shopping centres.

Numerous Data Sets

Data.gov.uk was launched in 2010 under the guise of non-personal open data. Today, it holds something 40,000 data sets (a data set is a single database table or a single statistical data matrix) and includes all manner of information collected from areas such as schools and families, Department for Health and so on.

On the 29 January 2010, **Boris Johnson**, former mayor of London, opened an online data warehouse containing more than 200 data sets just from London city authorities.

Today, for instance, the government knows you have visited www.truepublica.org.uk, the time you visited, how long you stayed, your IP address, and some information about your device. The law says they are not allowed to collect data on the pages read – but who knows. It also says they can't extract data from your device but they do as they've been caught doing it.

Each Internet Service Provider (ISP) and mobile carrier in the UK will have to store all these data sets, which the taxpayer will pay them to do, even though the taxpayer was never consulted. There is no judicial oversight, it'll be impossible to know when police target specific groups disproportionately. They are known to have illegally targeted law-abiding protestors, journalists, non-violent activists for instance.

Even More Intrusive

Just think about all this for a moment. You can't get away from a state snooper standing over you. But it is about to get much worse.

In July this year, the UK will become the first country in the world to bring in age checks for pornography online. Anyone visiting a porn website will be required to prove they are over 18. You may think that it is a good thing to be protecting our youngsters – but this is designed to lead somewhere else.

This is a set-up for what we at TruePublica have written about before – the creation of Digital ID cards. You will soon be hearing of a term called 'Robust Age Verification' (RAV). This is already different from Age Verification – itself to be legally rolled out in July this year. The RAV system is being piloted on those aged under 18. The Home Office is now already looking to add RAV technology for buying knives and alcohol and will extend it quite soon to vaping websites.

A similar system is now routinely in use for online gambling sites that started just two weeks ago.

Insiders have already stated that this same system is to be rolled out in Britain for using other online services in the future such as YouTube and Netflix. You might think this is outrageous, a conspiracy theory even – I promise you, it is the reality of what the government are allowing companies to do – and this, in turn, becomes a data collection point for the government.

One company, OCL is preparing to offer identity cards for students. It is already working with nightclubs and supermarkets and aiming to "own" the identity on their smartphones.

No Blunders

The mainstream media is starting to report that "***the government has quietly blundered into the creation of a digital passport – then outsourced its development to private firms, without setting clear limits on how it is to be used.***"

But they haven't blundered. This is all part of the overall desire to see the emergence of a digital ID card.

HMRC was recently told by the Information Commissioner to ditch millions of illegally collated voiceprints.

Further from collecting voiceprints, this state intervention into our lives has now extended to creating a biometric database, linked to a health database. These announced databases will hold the most private information imaginable about the civilian population of Britain. Fingerprints and facial recognition systems are just scratching the surface.

After the Windrush scandal, so serious that it saw the Home Secretary resign, you might have thought that the government would curtail its so-called 'hostile environment.' You'd be wrong – they doubled down without debate.

In January this year, an inspection report by the Independent Chief Inspector of Borders and Immigration (ICIBI) revealed Home Office ambitions to:

> "establish a system that obtains and shares an individual's immigration status in real time with authorised users, providing proof of entitlement to a range of public and private services, such as work, rented accommodation, healthcare and benefits."

It took this report to confirm that the Home Office is indeed building a massive hostile environment database for anyone with a background that is 'non-indigenous' – known internally as the "Status Checking Project".

Liberty said – this system "***could ostensibly be used to facilitate the sharing of personal data of any individual interacting with public services … amounting in effect to a digital ID card."***

This digital ID card will be online, you won't have access to it, but each time you want to use the NHS, send a child to a new school, accept benefits, go to the airport and so on, the state knows and builds its data set on you.

The government of Britain, using taxpayers money, have spent undisclosed billions building

the architecture of a secretive and terrifying surveillance state so intrusive it is no longer possible to escape its tentacles slowly wrapping itself around the face of civil society. In the not too distant future, there is nothing that law-abiding people will be able to do without the state snooper watching every move, waiting to approve your actions or worse still, penalise every minor infringement.

*

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

Featured image is from TP
