

The British Government's Secret Hostile Environment Database

By [True Publica](#)

Global Research, April 29, 2019

[TruePublica](#)

Region: [Europe](#)

Theme: [Intelligence](#), [Media Disinformation](#),
[Police State & Civil Rights](#)

Back in July 2011, David Cameron made a [speech about transparency](#). He told the electorate of Britain that a new dawn of government transparency had arrived and the release of official data would change the way government delivered public services.

“In so many ways, information is a national asset, and it’s time it was shared,” he said. “So today, we are making new commitments to transparency. What we’re proposing is something entirely different. Our aim is to provide similar information on performance right across the public services”

Cameron spoke eloquently about this “revolution in transparency” and the ‘profound impact’ it would have. What he didn’t say was that the government were also using an architecture of illegal surveillance tools as well. He didn’t say that the security services were taking images of you and your family (16 per cent of which were naked images or compromising in nature). He forgot to mention that every website you visited, every message you sent, every person you made contact with was logged and stored. His convenient amnesia included forgetting to mention operations [Tempora](#), [Echelon](#), [Optic Nerve](#) and other illegal mass surveillance systems. Or that the government was recording what news or other information subscriptions you paid, how and who you spent your money with, what sexual orientation you may be and any other personal information the state has no business knowing about.

Two years later the Edward Snowden revelations blew the lies of his government wide open. Now we had some real transparency. David Cameron then demonstrated his real passion for transparency by [warning and threatening](#) journalists that “*if they don’t demonstrate some social responsibility it will be very difficult for government to stand back and not to act.*” The state then forced their way into the offices of The Guardian and its henchmen from the security services destroyed the Snowden files and evidence it brought to light.

This state intervention into our lives has now extended to creating a [biometric database](#), linked to a [health database](#). To all intents, this represents nothing less than a national digital ID card system. National ID cards have been roundly rejected by the electorate and by parliament in the past – but that has not stopped this most secretive of governments.

All manner of government agencies, the people employed by them and the third party companies that design these systems – have access to your most private data. Tens of thousands of largely unknown people, many from foreign states have access (as the software is often designed by foreign companies).

After the unearthing of Theresa May's racist project of illegally and immorally ejecting black people from Britain in the [Windrush Scandal](#) – is it any surprise the government is secretly building a new surveillance architecture to sniff out any possibility of an immigrant not being quite good enough for Britain. Other than national security, and immigration is not an issue of national security, the only reason why the state does things in secret is that the electorate would not endorse their actions – or that they are illegal in the first place.

Secret establishment of new database

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, known internally as the “Status Checking Project”.

When, in autumn 2018, the Data Protection Bill included a sweeping immigration control exemption that would allow more or less any controller to set aside a person's data protection rights for immigration control purposes, Liberty, the human rights organisation were keen to find out exactly what the Government intended it to be used for. As Liberty [briefed](#) at the time, referencing a draft policy document [leaked](#) to the *Guardian*:

“this exemption 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.”

So there you have it. But Ministers remained curiously silent about the Status Checking Project. They insisted that the exemption would be used for tracking children of undocumented parents through their school records, or concealing the source of tip-offs to immigration enforcement (both things that can be done through existing crime-related exemptions to data protection law). The closest we had come before the ICIBI report to a public reference is a euphemistic mention of “new digital checking services” in the [Immigration White Paper](#).

The report also suggests that the system will be available to police in the future, despite ongoing concerns that overlap between policing and immigration enforcement is [undermining public safety](#).

Quietly entrenching the hostile environment

Liberty writes –

“The secrecy surrounding the so-called Status Checking Project is astonishing given that it has potentially huge human rights implications, both if it works, and if it doesn't.

It's one thing to send a text to someone telling them to leave the country, as happened in 2012, when the Home Office contracted Capita to send 39,000 texts to apparently undocumented migrants, some of whom were not, leading to a deluge of complaints. It's another thing entirely to communicate a person's status to landlords, employers, NHS providers, banks, police, and who knows who else, locking them out of the goods and services essential to a dignified life and the exercise of their fundamental rights.

That's what happens when the Home Office gets it 'right'. And that in itself is a serious problem. But the Home Office is also very likely to get things wrong. Its hostile environment data-sharing schemes already run with an [alarming error rate](#). Ten per cent of bank account refusals sampled during one inspection were found to have been made in error. In 2015, the DVLA was forced to reinstate more than 250 wrongly-revoked licences. And the Home Office has repeatedly refused to clean up its database on undocumented migrants, despite the National Audit Office and the ICIBI recommending that it does so."

The Windrush scandal exposed the devastating human impact of the hostile environment, as well as the Kafkaesque nightmare faced by people wrongly accused of being in the UK unlawfully. But it was not produced by a mere lack of documentation on the part of Commonwealth citizens. It was the product of a series of policy and legislative decisions that progressively stripped rights from a group of people who came to the UK as citizens and implemented a hostile environment despite [warnings](#) that those people might be locked out of essential services. In some cases, evidence that would have been useful to Windrush citizens was [destroyed](#), and extensive [evidence](#) that they provided was ignored on the grounds that it did not cover a few years out of decades.

Windrush proves the credentials of this government when it comes to discrimination. Illegal state surveillance proves the credentials of this government when it comes to the mass invasion of the state into our privacy. Now add both into the architecture of state control. What you start to see is a government willing to break all the rules, laws, ethics and all morality to pinpoint people, groups, communities, dissidents, protestors, organisations - in fact, anything it doesn't like and then deal with it in its own mendacious way.

This is all leading to one place and one place only. Behave according to the state (not necessarily by the laws of the land), or be punished by it.

Who gave the state the mandate to build a £multi-billion system to surveil our lives down to the tiniest detail? No-one did. The state did that all on its own. The building of this new database is yet another instalment of a state out of control. You might want to ask yourself if you're happy with where this is all going.

*

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

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