THE STATE OF SURVEILLANCE IN 2018

BIG BROTHER WATCH
DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

bigbrotherwatch.org.uk
@bbw1984

About Big Brother Watch

Big Brother Watch exposes and challenges threats to our privacy, our freedoms and our civil liberties at a time of enormous technological change in the UK.

We work to roll back the surveillance state and protect the rights of everyone in the UK to be free from unfair intrusion.

We campaign to protect freedoms in Parliament and through the courts. We produce unique research and investigations, and seek to educate and empower the public.

Big Brother Watch is a cross-party, non-party, independent non-profit organisation leading the protection of privacy and civil liberties in the UK.

In our pursuit for change, we use advocacy and campaigns; parliamentary lobbying; public interest litigation; research and investigations that inform policy and public debate; and public education and empowerment.

Contact

Silkie Carlo
Director
Email: silkie.carlo@bigbrotherwatch.org.uk

Jennifer Krueckeberg
Lead Researcher
Email: jennifer.krueckeberg@bigbrotherwatch.org.uk

24hr media line: 07505 448925

www.bigbrotherwatch.org.uk

Contents

Contributors

Kevin Blowe
NetPol

@copwatcher @PoliceMonitor

https://netpol.org/

Jen Persson
defenddigitalme

@The ABB @defenddigitalme

http://defenddigitalme.com/

Gracie Bradley
Liberty

@graciemaybe @libertyhq

https://www.libertyhumanrights.org.uk/

Tom Sanderson
Centre for Investigative Journalism

@cijournalism

https://tcij.org/

Phil Chamberlain
Author and journalist

@philchamberlain

Dr Jay Watts
Consultant Clinical Psychologist

@Shrink_at_Large

http://www.jaywatts.co.uk/

Ryan Gallagher
Journalist, The Intercept

@rj_gallagher @theintercept

https://www.rjgallagher.co.uk/

Ben Jaffey
Barrister at Blackstone Chambers

@benjaffey

Introduction

The extraordinary scale of surveillance in 2018 Britain affects all of us. Privacy is fast becoming a relic of the pre-internet age. We live in a time where our every step can be, and often is, recorded. Whilst the world's largest companies are profiting from tracking, analysing and quantifying every 'consumer', the state is building the most totalitarian style surveillance regime of any democracy in history under the Investigatory Powers Act 2016.

We have long warned of the harms of omnipresent surveillance to society as a whole - and this year, the risk that constant data collection poses to our democracy finally caused public concern after the Cambridge Analytical scandal. However, for some groups, the harms of normalised pervasive and intrusive monitoring practices are particularly tangible.

This report tells the experiences of those groups. It tells the stories of campaigners and unionists who are targeted by state surveillance simply for engaging in peaceful protest; of people too scared to access healthcare because of insidious government data sharing schemes; of welfare recipients afraid to reap the benefits of social media for fear their posts will be used against them.

The report details the growing normalisation of surveillance of children, preparing the next generation for monitoring and profiling - and reveals the ways in which this is already stigmatising vulnerable children.

This report also explores the damaging effects of zealous surveillance laws on two pillars of our democracy - journalism and law. In these first-hand accounts, the serious harm caused by the fading ability for even people in the most sensitive professions to communicate beyond the eye of the state becomes disturbingly clear.

The rapid emergence of new surveillance technologies is being matched by their fast and often lawless adoption by private companies and the state. Police forces can watch and track citizens without suspicion, increasingly using algorithms fed with personal information and data scraped from the internet to construct 'suspicion', assert 'risk', or even predict crime. Facial recognition cameras have crept onto our streets, making border style security and frequent identity checks a norm.

When the public voices concern about this growing authoritarianism, we are often told that if we have nothing to hide, we should have nothing to fear.

If you are reassured by that mantra, this report will make you think again.

Written in collaboration with renowned journalists, lawyers and activists, the report reveals the destructive impact surveillance has on people's lives, especially its effects on the most vulnerable in our society. Based on personal and professional experiences, the contributors illustrate how ever-present surveillance is not only eroding people's rights, but is damaging the very fabric of a free and democratic society. The report lays bare how life under the prying eye of authorities has created a chilling effect, suppressing people's willingness to speak out against wrongdoing and to be politically engaged.

Focusing on three areas, namely the rise of intrusive policing methods against targeted groups, the spectre of surveillance over sensitive professions, and increasing monitoring of vulnerable groups by public services, this report illustrates the impact of our shift to a mass surveillance society.

We hope that telling these stories will help us all to better understand the state of surveillance in 2018, the impact of abstract laws and policies on people's lives, and to find routes towards serious, radical change.

Targeted Groups in the Crosshairs

The 'chilling effect' of surveillance on the right to freedom of assembly

Kevin Blowe, Netpol

Kevin Blowe became Coordinator of the Network for Police Monitoring (Netpol) in 2014, when it began focusing on the policing of opposition to fracking across the country. He regularly contributes to the Organization for Security and Co-operation in Europe's work on protecting rights to freedom of assembly and spent 25 years as a campaigner with the Newham Monitoring Project in East London.

Netpol brings together many of the UK's most experienced activists, campaigners, lawyers and researchers to share knowledge and expertise. The network highlights and challenges disproportionate or excessive policing that violate the rights to freedom of assembly and expression. Netpol works in partnership with independent front-line groups, to address the lack of a cohesive voice for these groups within the mainstream discourse around civil liberties.

The right to freedom of assembly is protected by national and international human rights law. For a number of years, Netpol has worked with organisations like the Organisation for Security and Cooperation in Europe (OSCE) to help refine guidelines on assembly rights and to highlight, in particular, how confrontation policing, the misuse of force and mass arrests are not the only factors likely to have a 'chilling effect' by actively discouraging people from taking part in peaceful protest. So too does the use of sophisticated and intrusive surveillance to target individual activists, campaign groups and even entire social and political movements.

Public order policing in the UK is intelligence-led and the standard is set out in the National Intelligence Model[1] that was developed in 2000 by

1 National Criminal Intelligence Service (2000):The National Intelligence Model. Available at: http://www.intelligenceanalysis.net/National%20Intelligence%20Model.pdf

the National Criminal Intelligence Service (now part of the National Crime Agency). Central to the model is the creation and use of personal profiles to "provide a detailed picture of the (potential) offender and his associates for subsequent action", including "habits, lifestyle, modus operandi, addresses, places frequented, family-tree chart, photographs, risk to public, ability to protect him/herself, and related information."[2]

The problem, however, is that UK police have treated legitimate campaigning activities in a similar way to their response to organised criminal networks: by building profiles on the size, structures, leadership and alliances of campaign groups, by singling-out 'organisers' for particular attention, by visiting campaigners at home[3], filming attendance at meetings and protests and by routinely monitoring social media.

> ***UK police have treated legitimate campaigning activities in a similar way to their response to organised criminal networks: by building profiles on the size, structures, leadership and alliances of campaign groups***

The National Intelligence Model also identifies a "control strategy" with resources allocated for intelligence, prevention and enforcement, with particular emphasis on "disruption" and "network demolition". Since Netpol was founded in 2009, individual campaigners have repeatedly expressed to us their concerns about personal targeting or being 'picked out' after having their photograph taken, facing identification checks by police during a stop and search and police officers publicly naming them. We have had numerous reports of activists and even volunteers helping refugees being detained, interviewed and searched under Schedule 7 of the Terrorism Act 2000 at ports and airports.[4]

Campaigners have also told us how obvious or conspicuous surveillance alienates people from others, including communities they are trying to connect or engage with by creating the impression that they are criminals or 'trouble'. Campaigners have also said they believe surveillance is intentionally divisive, calling attention to those who are allegedly 'aggressive' or whom the police want to isolate or alienate from other protesters.

2 Ibid., p.18.
3 Netpol (2015): Why are counter-terrorism police treating fracking opponents as 'extremists'? Available at: https://netpol.org/2015/04/09/prevent-fracking-extremism/
4 Stone, J. (2015): Police use anti-terrorism powers to detain UK volunteers taking aid to Calais refugee camp, The Independent, 6 November. Available at: https://www.independent.co.uk/news/uk/politics/police-use-anti-terrorism-powers-to-detain-british-volunteers-taking-aid-to-calais-refugee-camp-a6724221.html

Domestic extremists

This fear that police surveillance is concerned less with actual criminal behaviour and more with disruption based on subjective political judgements is fuelled by the way the police have claimed a broad and diverse range of campaigners are "domestic extremists".

This label has no basis in law and its definition has changed often since it appeared in 2004. It first came to national prominence in 2009 when the Guardian reported on how surveillance was used to police peaceful environmental protests at the Drax power station in North Yorkshire three years earlier.[5] However, it was the exposure in 2011 of the undercover police officer Mark Kennedy that led to far greater concerns about the scale of surveillance of campaigners and eventually to the setting up of the Undercover Policing Inquiry in 2015.[6]

Of equal concern is the extent of data retention on various national "domestic extremism" databases. In 2014, the Green Party peer and former Deputy Mayor of London, Baroness Jenny Jones, discovered her personal details had been included on the database[7] – administered by the Metropolitan Police, over whom she had had an oversight role – and subsequently that they had deliberately destroyed records to cover up its surveillance on her.[8] The same year, a campaigner discovered that police had been carrying out surveillance on political campaigners while they were at the Glastonbury festival[9] and the police disclosed that I too had been labelled a "domestic extremist", despite having no criminal record, because of involvement in campaigning around security and the 2012 Olympics.[10] In 2015, another Green Party politician, Ian Driver, who was standing as a parliamentary candidate in Kent against former UKIP leader Nigel Farage, found out that he had been monitored by police for over four years.[11]

Despite the many concerns it raised, the "domestic extremism" label has, nevertheless, proved convenient for the police in providing a justification for the scale of intelligence-gathering on political dissent. In particular, it has been utilised to obscure from public scrutiny the involvement of counter-terrorism officers in the government's secretive Prevent programme.

---

5 Evans, R.; Lewis P. and Taylor M. (2009): How police rebranded lawful protest as 'domestic extremism', The Guardian, 25 October. Available at: https://www.theguardian.com/uk/2009/oct/25/police-surveillance-protest-domestic-extremism

6 Evans, R. and Lewis P. (2011): Undercover officer spied on green activists, The Guardian, 9 January. Available at: https://www.theguardian.com/uk/2011/jan/09/undercover-office-green-activists

7 Cox, J. (2014): London's Police Database of Extremists Also Includes Politicians and Activists, Motherboard, 16 June. Available at: https://motherboard.vice.com/en_us/article/mgb3va/londons-database-of-extremists-also-includes-politicians-and-activists

8 Evans, R. (2017): Inquiry over Met police intelligence unit claimed to have destroyed files, The Guardian, 8 February. Available at: https://www.theguardian.com/uk-news/2017/feb/08/inquiry-over-met-police-intelligence-unit-claimed-to-have-destroyed-files

9 Evans, R. and Lewis P. (2012): Glastonbury festival: how police spied on political campaigners, The Guardian, 15 July. Available at: https://www.theguardian.com/music/2012/jul/15/glastonbury-festival-police-spy-operation

10 Netpol (2014): Secret Diary of an Olympic Domestic Extremist, 5 February. Available at: https://netpol.org/2014/02/05/olympic-domestic-extremist/

11 https://www.theguardian.com/uk-news/undercover-with-paul-lewis-and-rob-evans/2015/may/01/police-monitored-political-movements-of-candidate-standing-against-nigel-farage

Since 2014, Netpol has organised an annual Domestic Extremist Awareness Day to highlight the negative impact of the police obsessively searching for and monitoring so-called 'extremists' amongst campaigners and activists, and to support the UN Special Rapporteur's call in 2013[12] (repeated in 2016[13]) for authorities to "instruct police officers that peaceful protestors should not be categorised as domestic extremists".

We have highlighted the significant obstacles campaigners face to find out whether they have been labelled an extremist or to challenge the inaccuracy of information held about them. We also intervened as an interested party in the UK Supreme Court appeal case of Brighton protester John Catt – a case that resulted, controversially, in judicial approval for the mass surveillance of UK political activism.[14] After legal proceedings lasting two years, Netpol managed in 2018 to successfully challenge the police at an Information Tribunal and force them to confirm that anti-fracking campaigners had been referred to a project for people deemed "vulnerable to radicalisation".[15]

Anti-fracking

In our work supporting the anti-fracking movement, we have documented how campaigners engaged in peaceful direct action have been included in Prevent training for public sector staff as examples of an alleged extremist threat. For example, in September 2015, it emerged that a Prevent training session organised by West Yorkshire Police for teachers gave the arrest of Green MP Caroline Lucas at an anti-fracking protest in Sussex as an example of extremism[16] (it was subsequently revealed that Lucas had been regularly tracked by domestic extremism unit officers[17]). We have also raised concerns about how labelling opponents of the onshore oil and gas industry is likely to drive decisions about potentially deploying undercover police officers (in 2016 the National Police Chiefs Council refused to rule this out, saying "any tactic, including covert tactics, is for the policing commander for the operation"[18]).

In December 2016, the Home Office was finally forced to issue a statement saying "support for anti-fracking is not an indicator of vulnerability" to

12 UN News (2013): United Kingdom must review measures affecting right to peaceful assembly – UN expert, 23 January. Available at: https://news.un.org/en/story/2013/01/430492-united-kingdom-must-review-measures-affecting-right-peaceful-assembly-un-expert
13 Freeassembly.net (2016): Statement by the United Nations Special Rapporteur on the rights to freedom of peaceful assembly and of association at the conclusion of his second visit to the United Kingdom, 21 April. Available at: http://freeassembly.net/news/statement-united-kingdom-follow-up/
14 Netpol (2015): Analysis of the UK Supreme Court ruling on surveillance of political activism, 5 March. Available at: https://netpol.org/2015/03/05/analysis-supreme-court-catt-ruling/
15 Netpol (2018): Victory for Netpol in legal challenge over scale of surveillance on anti-fracking campaigners, 11 June. Available at: https://netpol.org/2018/06/11/prevent-tribunal-victory/
16 Bloom, A. (2015): Police tell teachers to beware of green activists in counter-terrorism talk, 4 September. Available at: https://www.tes.com/news/police-tell-teachers-beware-green-activists-counter-terrorism-talk
17 Evans, R. and Dood, V. (2016): Police anti-extremism unit monitoring senior Green party figures, The Guardian, 28 April. Available at: https://www.theguardian.com/politics/2016/apr/28/police-anti-extremism-unit-monitoring-green-party-caroline-lucas-sian-berry
18 Netpol (2016): Police refuse to rule out using undercover officers at anti-fracking protests, 17 August. Available at: https://netpol.org/2016/08/17/npcc-extremism-spycops/
19 Townsend, M. and Cobain, I. (2016): Home Office forced to defend anti-fracking groups from extremism claims, The Guardian, 10 December. Available at: https://www.theguardian.com/uk-news/2016/dec/10/home-office-defends-anti-fracking-groups-extremism-claims-prevent

extremism,[19] after press coverage about City of York Council[20] and a school in Driffield in North Yorkshire[21] including anti-fracking campaigns in their counter-terrorism advice.

Counter-terrorism

However, in September 2017, 'Counter Terrorism Local Profiles' developed by the police under the government's Prevent strategy were released and identified protests at Broadford Bridge in Sussex as a "priority theme... where increased tensions or vulnerabilities may exist".[22] A similar profile for Surrey highlighted "community tensions related to onshore oil and gas operations" in the east of the county. Protests in both areas did not start until months after the Home Office gave assurances to anti-fracking campaigners that it would no longer collectively treat them as a "domestic extremist" threat.

In fact, since the first revelations about the scale of secretive surveillance on hundreds of campaign groups led to a public inquiry, the national unit formerly responsible for "domestic extremism" has been subsumed into the police's nationwide Counter Terrorism Network. This means that it is far more difficult to obtain disclosure of information about so-called 'extremism' related to protest because it is treated, in effect, like terrorism.

This matters for individual campaigners because the Metropolitan Police's own policy on the creation of 'nominal files' on its secret databases acknowledges that a person identified as a subject of interest is treated differently "over and above people named in general intelligence records".[23] The consequence is that any interaction a person affected has with the police, whether or not at a protest, is likely to flag up that the person is a subject of interest.

We believe without any meaningful definition of what "domestic extremism" means, the label threatens the growth and development of civil society and justifies a range of intrusive monitoring tactics and repressive policing measures.

The impact

Monitoring of entirely peaceful demonstrations already indicates that campaigners taking part in them are far more likely than the population

19 Townsend, M. and Cobain, I. (2016): Home Office forced to defend anti-fracking groups from extremism claims, The Guardian, 10 December. Available at: https://www.theguardian.com/uk-news/2016/dec/10/home-office-defends-anti-fracking-groups-extremism-claims-prevent
20 The BBC (2016): City of York Council's anti-fracking terrorism links 'ludicrous', 5 December. Available at: https://www.bbc.co.uk/news/uk-england-york-north-yorkshire-38213179
21 Barnett, B. (2016): Driffield headmaster sorry for linking anti-fracking to Islamic State in school newsletter, The Yorkshire Post, 02 December. Available at: https://www.yorkshirepost.co.uk/news/driffield-headmaster-sorry-for-linking-anti-fracking-to-islamic-state-in-school-newsletter-1-8271878
22 CAGE (2017): PREVENT is about Policing Dissent not Safeguarding, 7 September. Available at: https://www.cage.ngo/prevent-is-about-policing-dissent-not-safeguarding
23 The Metropolitan Police (2013): National Domestic Extremism & Disorder Intelligence Unit. NDEDIU Nominal Creation Policy. , p. 4

in general to face arrest and therefore to have their biometric data (facial characteristics, fingerprints or DNA) recorded and retained. Even if, as is regularly the case, they are never charged with an offence, it is unlikely all this data is ever deleted.

There is also heard testimony from campaigners that suggests police are continuing to compile datasets from routinely tracking the movement of vehicles at protests and photographing anyone associated with protest groups, without the need to demonstrate a reasonable suspicion of involvement in crime. This was reported on as far back as 2009[24] and Netpol has witnessed it at protests against fracking in Cheshire and Lancashire. As well as automated tracking using ANPR (Automatic Number Plate Recognition) technology, this year we have also observed the police openly deploying automated facial recognition surveillance at an anti-arms fair protest for the first time.

The impact of such data gathering and retention is extensive. On top of the issues already highlighted, we have documented evidence that campaigners involved in public assemblies are more likely to face vehicle stops and interference in matters unrelated to protest (in several instances, for example, farmers in Lancashire who were arrested for minor offences at anti-fracking protests found that their shotgun licences were revoked without explanation – and in one instance, a shotgun was collected by armed officers).

Netpol has long argued that this intense focus on surveillance provides as much of a 'chilling effect' on the freedom to protest as any confrontational policing at a protest itself: it is just as likely to discourage many from participation in campaigning activities. It has also significantly shifted operational priorities, leading police commanders to prioritise intelligence gathering over negotiation or mediation; and it influences officers' discretion in favour of making arrests as an opportunity to obtain information on individuals. It has significantly compromised, for example, the credibility of Police Liaison Officers, whose role is supposedly to facilitate protest but who are widely treated with suspicion by most campaigners.[25]

Key to all these concerns is the question of privacy in the gathering of data by the police and the inappropriate use of counter terrorism powers.

Much debate on privacy and the gathering and retention of data remains overwhelmingly focused on individual rights. This overlooks the additional negative impact of surveillance when applied to an entire group, and an entire democratic mechanism. The excessive surveillance of activists inhibits collective discussion, decision-making and organisation, which are fundamental to the ability of campaigners to exercise their rights to protest effectively. We must consider the impact of this surveillance on our democratic rights and society as a whole.

24 Lewis P.; Evans R.(2009): Activists repeatedly stopped and searched as police officers 'mark' cars, The Guardian, 25 Oct. Available at: https://www.theguardian.com/uk/2009/oct/25/surveillance-police-number-plate-recognition

25 See: https://netpol.org/police-liaison-officers/

Blacklisting: the secret habit employers can't seem to kick

Phil Chamberlain, journalist and author

Phil Chamberlain is the Head of Department of Film & Journalism at the University of the West of England where he is responsible for more than a dozen undergraduate and postgraduate programmes as well as the Digital Cultures Research Centre. He teaches investigative journalism and his research interests cover surveillance, corporate discourses and court reporting.

Phil has 20 years' experience as a freelance journalist with working for newspapers, magazines and NGOs providing investigative news and feature stories. He co-authored Blacklisted: the secret battle between big business and union activists and is the author of Drones and Journalism: how the media is making use of unmanned aerial vehicles.

In 1987, Conservative MP Ken Warren wrote to Prime Minister Margaret Thatcher attaching a list of 270 names of alleged members of the left-wing organisation Militant.[26] He demanded the security services investigate to ensure that none of those on the list were placed in sensitive positions in the civil service.

Warren's McCarthyite intervention piqued the interest of a secret Whitehall committee called Subversion in Public Life (SPL). Made up of senior civil servants from different departments along with MI5 and Special Branch representatives, SPL analysed the supposedly subversive threat to the machinery of government.

While Warren may have worried about 270 alleged Militant members, the committee noted that his list "added little to our present knowledge; indeed it contains a number of known inaccuracies."[27] A report from the committee the previous year had estimated there were 50,000 potential subversives in the country and identified 1,420 who worked in the civil

26 Cabinet Office paper 301/486 Subversion in Public Life 1987 Jan 27 - 1989 July 7
27 ibid
28 Cabinet Office paper 301/485 The threat of subversion in the UK 1982 Feb 19 - 1986 Mar 18. See also Cobain, I (2018) Subversive civil servants blacklisted under Thatcher The Guardian https://www.theguardian.com/uk-news/2018/jul/24/subversive-civil-servants-secretly-blacklisted-under-thatcher

service.[28] The majority of these were members of left-wing organisations but far right supporters were also listed along with members of anarchist groups and "black and Asian racial extremists".[29] The Department of Health and Social Security recorded the biggest number of subversives within its ranks with 360 (including six fascists).[30] The perceived infiltration of civil service unions by these groups was a constant source of concern. Margaret Thatcher asked that the SPL also look into local government, education and the NHS which proved more problematic because of the devolved nature of those organisations. One solution was that education inspectors were asked to supply MI5 with details on teachers.

The SPL was not merely a bureaucratic exercise but a blacklist. Departments were encouraged to not only record these individuals but ensure they were not put in sensitive roles or moved to posts where they could be isolated. There is no indication the individuals were ever informed about their status; indeed the chairman of the SPL warned of the intense embarrassment if its activities became public knowledge.

In 1985, the same year the SPL began its work, it had been revealed that the BBC was running a secret political vetting operation with MI5.[31] Meanwhile the Economic League, again with close links to the security services, was at the height of its powers even if its veil of secrecy was slipping. It was paid by corporations to keep files on hundreds of thousands of people deemed subversives and to ensure they could not get employment.

The SPL was apparently wound up in 1988 and the Cabinet Office has refused to comment further other than to say that it is an historical matter.

But blacklisting is the employment habit the UK cannot seem to kick.

Building firm boss Cullum McAlpine was keen not to let blacklisting resources go to waste. He paid £10,000 to the Economic League for several thousand personal files covering the construction sector and set up one of the league's investigators and an admin assistant in a discrete office in the West Midlands.[32] Until it was exposed in 2009, his organisation the Consulting Association was taking thousands of pounds in fees from the country's biggest building firms to run a secret blacklisting operation.[33]

Engineer Dave Smith was one of the workers on the firm's files and his experience is typical. What initiated his file was taking part in action to recover unpaid wages and becoming a safety representative - in other words, legitimate trade union activity. The file details what car he drove, his

29 Ibid 301/485
30 Ibid 301/485
31 Hollingsworth, M and Norton-Taylor, R (1988) Blacklist: the inside story of political vetting London: Hogarth Press p91-121
32 Smith, D and Chamberlain P (2016) Blacklisted: the secret war between big business and union activists Oxford: New Internationalist p168
33 Evans, R and Chamberlain P (2009) Firms brought secrecy persona data on staff – privacy chief The Guardian https://www.theguardian.com/uk/2009/mar/06/data-protection-construction-industry

family members, as well as jobs he applied for. The result was immediate and catastrophic; work dried up and Dave was eventually forced to leave the industry. He never knew his file existed until the Information Commissioner raided the Consulting Association, seized some of its material and then made it available to the subjects. Dave's story is repeated many times over but often with worse results. Marriages broke up under the strain of financial insecurity, people were forced to move abroad and their health was affected.

It appears that one feature of such operations is their tendency to expand. Just as the SPL was asked to look into local government and schools, the Economic League had considered keeping lists of football hooligans and people with HIV. The Consulting Association was not limited to the construction sector but had files on people working in local politics, academia, journalism, the railways and the offshore oil industry. The latter sector had a notorious policy called 'Not Required Back' which was stamped on the files of many a trade union member who had spoken out.[34]

> ***Far from an historic concern and one limited to particular trades, the monitoring and blacklisting of workers remains the dirty secret of UK labour relations***

The Consulting Association also had files on several hundred environmental activists and here the overlap between the private sector and the state was most explicit. Along with anti-fascist activists, environmental activists were of particular interest to the security services. An officer in one of the police's surveillance units even gave a presentation on its work targeting animal rights groups to the Association. The files, along with evidence from police whistleblower Peter Francis, have revealed that undercover police officers infiltrated trade unions, black justice campaigns and environmental groups among others. Francis was a member of the Special Branch's Special Demonstration Squad (SDS) set up in 1968 and which only folded after being exposed in 2008. Some SDS officers had sexual relations with activists and even children in the course of intruding on and manipulating activists' lives.

After reviewing evidence from the files and other sources, the Blacklist Support Group complained to the Metropolitan Police in 2012 with six specific allegations about collusion between the state and the private sector. In 2018 the Metropolitan Police finally admitted, "Sections of the policing community throughout the UK had both overt and covert contact

34 Smith, D and Chamberlain P (2016) Blacklisted: the secret war between big business and union activists Oxford: New Internationalist p106
35 Letter from Richard Martin, Deputy Assistant Commissioner, Metropolitan Police Service to Christian Khan Solicitors 15 February 2018. See also Casciani, D (2018) Metropolitan Police admits role in blacklisting construction workers BBC https://www.bbc.co.uk/news/uk-43507728

with external organisations, including the Economic League, for reasons stemming from crime reporting and the maintenance of public order and the prevention of terrorism."[35] This statement only acknowledged what had become incontestable. However, the Metropolitan Police rejected other complaints and specifically exonerated the Special Demonstration Squad from colluding with blacklisters.

The police's statement deployed a well-worn defence for blacklisting operations - that they are about crime or terrorism. The Cabinet Office files on the Subversion in Public Life committee explicitly separated out actions to counter terrorism from its remit and made no claim to tackle illegal behaviour. An analysis of the Consulting Association files shows that time and again, the first activity to trigger monitoring was an individual raising health and safety concerns. It was legitimate union activity that resulted in people being surveilled - criminal activity was mentioned in only a handful of the more than 3,000 files it held. [36]

It is worth noting that the activities of the SDS, the Consulting Association and the Economic League only ended after public exposure. There is little sense of a culture that sees such operations as wrong; only in getting caught. It took seven years for blacklisted construction workers to win a financial settlement and only one person was ever punished by the courts for their role in the scandal. The SDS' activities are currently the subject of a judge-led inquiry which is into its third year but yet to even begin taking evidence. Without an effective inquiry that the people affected can trust, there is little chance of change or indeed justice.

Meanwhile, the monitoring of workers, unionists and especially whistleblowers continues. In 2015, Sir Robert Francis QC produced "Freedom To Speak Up", a report into whistleblowing in the NHS.[37] Francis reported that many people spoke of fears that whistleblowing would have a detrimental effect on their career and that there was evidence of "vindictive treatment" of people who raised concerns.

> ***The suppression of staff who speak up is a very old problem and will not go away until decision makers truly accept that it is better to run a service in which staff and patients have a voice,***

36 Smith, D and Chamberlain, P ibid
37 Francis, R (2015) Freedom to speak up: an independent review into creating an honest and open reporting culture in the NHS http://freedomtospeakup.org.uk/the-report/
38 Details on Dr Alexander's evidence to parliament on her experiences can be found here https://minhalexander.com/about/. A video of her talk to the University of Greenwich conference can be found here https://www.youtube.com/watch?v=doDKGnAVs6c
39 One of a number of NHS cases studies quoted in Martin,D, Allen, V and Marsden,R (2016) Whistleblowers out in the cold Daily Mail http://www.dailymail.co.uk/news/article-3441517/Whistleblowers-cold-Struggling-work-isolated-shunned-terrible-price-medics-sacked-exposing-NHS-failures-paying.html
40 See http://www.compassionincare.com/

Dr Minh Alexander worked for 14 years as a consultant psychiatrist and had raised concerns over certain medical practices. She was made redundant in 2013 and reached a settlement with her employer.[38] Alexander is one of many NHS staff who fear their careers have been ended because their decision to raise concerns has been recorded and shared. "The suppression of staff who speak up is a very old problem and will not go away until decision makers truly accept that it is better to run a service in which staff and patients have a voice," Alexander said.[39] Similarly, Eileen Chubb was forced to quit her job as a care assistant after raising concerns about patient safety. She now runs Compassion in Care which campaigns for better care for the elderly.[40] Official figures for 2017/18 showed that more than 350 whistleblowers in the NHS experienced repercussions after coming forward, including negative effects on their careers.[41] Meanwhile, the Care Quality Commission, which helps regulate the sector, has been accused of revealing the details of dozens of whistleblowers to employers - a claim it denies.[42]

Far from an historic concern and one limited to particular trades, the monitoring and blacklisting of workers remains the dirty secret of UK labour relations.

In one of the final acts of the Brown government, blacklisting was made illegal in 2010. As with pretty much every other state attempt to deal with the issue, it was a failure. Employment expert Professor Keith Ewing from King's College London set out at length why the regulations are full of holes.[43] A key flaw is that it is a civil rather than criminal offence with the onus on the victim to prove their case; and since the victim is often up against a corporation, the balance of power is firmly against them. Blacklisting is a stark reminder of that imbalance of power but also that there is often no line between state and private, corporate and civil. The undercover police officers manipulating female activists into relationships were often seeking to protect corporate interests rather than prevent criminal wrongdoing. Indeed, in some cases, it is alleged they acted as agent provocateurs to incite wrongdoing.[44]

There are three areas that desperately need improvement in order to tackle this scandal.

Firstly, we need a properly funded public inquiry that can tease apart the links between the various people involved in blacklisting. Too much of the information has had to be pieced together by a few journalists, lawyers, MPs and many campaigners. Theresa May launched the judge-led Undercover Policing inquiry[45] following revelations about the Special Demonstration

41 Matthews-King, A (2018) Hundreds of whistleblowers claim they faced recriminations as NHS fears repeat of Gosport scandal The Independent https://www.independent.co.uk/news/health/gosport-scandal-latest-inquiry-jane-barton-whistleblowers-deaths-war-memorial-hospital-a8410761.html
42 Hosken, A (2017) Health regulator reveals whistle-blowers to employers BBC https://www.bbc.co.uk/news/uk-politics-42314351
43 See for instance http://www.lrd.org.uk/issue.php?pagid=100&issueid=1508
44 Evans, R (2016) Met to investigate claims undercover officer set fire to Debenhams store The Guardian https://www.theguardian.com/uk-news/2016/apr/20/met-opens-inquiry-after-claims-undercover-officer-set-fire-to-shop
45 See https://www.ucpi.org.uk/
46 Evans R, and Lewis, P (2013) Undercover: the true story of Britain's secret police London: Faber and Faber

Squad broken first by The Guardian.[46] It has been little more than a disaster with no evidence heard in its first three years and participants boycotting the process because of a lack of trust. It is not expected to report until 2023.

Secondly, organisations charged with protecting personal information need better resourcing. Without the Information Commissioner's Office the secret blacklist files would not have been made public. The ICO needs the toughest tools if it is going to take on the biggest state and corporate interests and their digital archives.

Thirdly, we need to see the delivery of justice. It is worth pointing out that only one person was ever convicted for their part in the scandal. The company directors, human resources managers, police officers, civil servants and regulators who authorised, ignored or participated received no sanction. A survey by Building magazine found that 78% of human resources officials named as complicit in blacklisting were still employed four years after their role was revealed.[47] There is a culture of acceptance that secret political surveillance and the sharing of information has always been with us and always will. Changing that culture will require a change in how power is distributed in society. It sounds too ambitious an objective.

However, in 2009 a few dozen people affected by the blacklist gathered in a room by Parliament and decided that they wanted to do something about it. Seven years later they forced a multi-million pound settlement from transnational construction firms.

Where do we want to be in the next seven years?

47 Hurst, W (2013) Blacklisting: human impact Building http://www.building.co.uk/analysis/news-analysis/black-listing-human-impact/5055579.article

Risks for Sensitive Professions

The impact of UK state surveillance on investigative journalism

Tom Sanderson, Centre for Investigative Journalism

Tom Sanderson is the Acting Director of the Centre for Investigative Journalism. He joined in 2014 to manage training provision and develop projects. His most recent work has focused on supporting new models of community and non-profit journalism with investigative training.

The Centre for Investigative Journalism is a think-tank, alternative university and an experimental laboratory set up to train a new generation of reporters in the tools of investigative, in-depth, and long-form journalism across all media. Registered as a charity, we robustly defend investigative journalists and those who work with them.

A key revelation of the Snowden documents was the confirmation that investigative journalists are firmly in the crosshairs of state surveillance mechanisms. One restricted document stated: 'journalists and reporters representing all types of news media represent a potential threat to security',[52] adding: 'Of specific concern are "investigative journalists" who specialise in defence-related exposés either for profit or what they deem to be of the public interest'.

If we accept that there is any kind of watch-dog role for investigative journalism in providing access to information for public scrutiny, or that the legal definition of 'public interest' which journalists work to is at all valid, then this represents a serious threat to the functioning of our democracy.

The suppression and deterrence of investigative journalists in conducting their work by elements of the state is of course nothing new. However, legislation such as the Regulation of Investigatory Powers Act 2000 (RIPA), followed by the Investigatory Powers Act 2016 (IPA) - coupled with the

52 Ball, J. (2015): GCHQ captured emails of journalists from top international media, The Guardian, 19 January. Available at: https://www.theguardian.com/uk-news/2015/jan/19/gchq-intercepted-emails-journalists-ny-times-bbc-guardian-le-monde-reuters-nbc-washington-post

growing sophistication, reach and affordability of surveillance tools – means that ever more powerful tools are in the hands of those who seek to cover up wrongdoing or persecute journalists and their sources.

The assault continues. The Law Commission's proposals for a new 'Espionage Act'[53] would deliberately blur the distinction between information-seeking investigative journalists and spies working on behalf of a hostile state, feeding into an already dangerous public narrative which surrounds the journalism industry.

A further danger is represented by the extension of surveillance tools and practice to non-state actors who may be subjects of journalistic investigations such as corporate interests or organised crime. State-driven trials and investment in new forms of surveillance such as 'IMSI catchers', facial recognition software, and state-required storage of 'internet connection records' open up the possibility of journalists and sources being compromised by even less accountable bodies than state security services.

Though the actual monitoring of journalists in the normal course of their work is a major threat, the primary danger inherent in the UK's increasingly draconian legislative context is the chilling effect it has on the industry and on wider society in general.

At the Centre for Investigative Journalism we are in frequent contact with journalists working to provide scrutiny on matters of public interest and we have seen a marked increase in concerns around becoming a target for security services, driven in large part by the rhetoric around surveillance and backed up by the regressive changes to legislation. We produced a handbook titled 'Information Security for Journalists' on surveillance protections for journalists, which has been downloaded over 270,000 times since its publication in June 2014. We also modify laptops and produce anonymising operating systems for high risk investigative journalists. In fact, we have witnessed it become commonplace for journalists to be comfortable using security tools such as the anonymising Tor browser, the Signal app for encrypted communications, PGP encrypted emails, and even signal-blocking Faraday cages for phones, despite the significant inconvenience such measures can cause. We are aware that some investigative journalists working on particularly sensitive projects, whether freelancers or those at major newsrooms, go to considerable lengths to keep important communications entirely offline, including by using secondary 'air-gapped' laptops isolated from internet connections to mitigate the risk of remote State hacking. Journalists working on the Snowden documents even had to work in sealed rooms, which blocked incoming and outgoing signals.

With threats emerging at a rapid pace, we now produce short videos on information security for journalists. Our trainers have assisted multiple news organisations, international media conferences, and hundreds of

53 The Law Commission (2017): Protection of Official Data – A Consultation Paper. Available at: http://www.lawcom.gov.uk/app/uploads/2017/02/cp230_protection_of_official_data.pdf

journalists with cybersecurity training. We find it deeply concerning that there is such demand, and evidently such need, for this training among UK journalists reporting on UK issues.

The chilling effect on journalism that we have witnessed is impossible to quantify - we cannot know how many whistleblowers will decide not to contact journalists for fear of their identity becoming known. The mass retention of communications data practiced in the UK under the IPA is especially harmful to journalists, who have an ethical obligation to protect the identities of their sources and whistleblowers, especially those who wish to remain anonymous.

The chilling effect on journalism that we have witnessed is impossible to quantify - we cannot know how many whistleblowers will decide not to contact journalists for fear of their identity becoming known.

The awareness that every communication leaves a digital trace, which is highly likely to be stored under a government IPA notice, means that it is almost impossible for a journalist to communicate with a source in total confidence – especially in absence of serious security tools. In addition, the tracking of location data makes it incredibly difficult for journalists to meet sources with an assurance of confidence. In a 2017 report titled "Protecting Sources and Whistleblowers in a Digital Age"[54] the Institute of Advanced Legal Studies warned:

> *"Technological change means that journalists, freelancers and publications are faced with previously unprecedented difficulties in protecting their sources (...) Although a number of domestic and European legal protections exist for the protection of confidential sources, their effectiveness is considerably weakened by technology that provides an easy route to information; and the use of covert powers to which journalists and sources may be oblivious.*
>
> *Working investigative journalists and media lawyers, many with several decades of experience, are profoundly concerned about the growing technological and legal vulnerability of confidential sources including whistleblowers, the protection of whom is essential to the pursuit of responsible journalism in the public interest."*

This closely reflects the experience and analysis of the Centre for Investigative Journalism in 2018.

54 Protecting Sources and Whistleblowers in a Digital Age – Information Law and Policy Centre, Institute of Advanced Legal Studies, 22 February 2017, p.4: http://infolawcentre.blogs.sas.ac.uk/files/2017/02/Sources-Report_webversion_22_2_17.pdf

Ultimately, the problems of an overzealous surveillance regime go far deeper than censorship when the perceived risk of serious investigations compels journalists to effectively self-censor their work and decide to avoid potentially controversial or counter-narrative research. Some of the most important revelations uncovered by journalists in UK history may never have come to light and the wrongdoing uncovered therefore would have stood little chance of ever being rectified if the current climate had been in place. For this reason, the current state of surveillance risks not only obstructing whistleblowers and chilling investigative journalism – it has the potential to stall social change.

A personal experience: Investigative Reporting in the UK and the Surveillance Chilling Effect

Ryan Gallagher, Journalist (Intercept)

Ryan Gallagher is a UK-based investigative reporter and editor for The Intercept. His work focuses on the intersection between national security, counter-terrorism, technology, and human rights.

Perhaps the most important aspect of any journalist's work is the ability to communicate confidentially with sources. Whistleblowers who have information about criminality or abuses of power need to feel that they can contact a journalist and that in doing so their identities will be protected.

Unfortunately, the Investigatory Powers Act, which forces all internet and phone companies to store logs of every communication they process, makes sources feel less safe. It creates a chilling effect – and means whistleblowers are less likely to come forward. There are encryption and anonymity tools that we as journalists can use to protect our sources. But these do not cancel out the chilling effect, because some sources will still be deterred. That means the public loses out: important information that should be exposed stays secret, and abuses do not get reported.

The Investigatory Powers Act contains clauses that are supposed to protect journalists' confidential communications with their sources. However, police and other authorities' requests to review call or internet records are made in secret. News organisations are not notified and therefore have no chance to challenge the demands for their journalists' or their sources' private data. We instead have to put blind faith in a "judicial commissioner" to decide when it is and is not appropriate to allow the state to identify our sources. For me that is a serious concern.

> ***This means the public loses out: important information that should be exposed stays secret, and abuses do not get reported.***

The threats that we face are not hypothetical. Between 2012 and 2015, under the Regulation of Investigatory Powers Act, which has since been replaced by the Investigatory Powers Act, police tried on more than 600 occasions to use surveillance powers to identify journalists' sources.[55]

Other laws pose threats to press freedom. Especially in the field of national security reporting, it is routine to deal with sensitive information, which is sometimes classified. Back in 2013, when the US National Security Agency whistleblower Edward Snowden leaked a trove of documents about government mass surveillance, the British government's response was to try and stop journalists reporting on the secret files. Police – in coordination with MI5 – used the Terrorism Act to seize an encrypted set of the documents; weeks earlier, the government had also forced The Guardian to destroy copies of them in London.

After those incidents, I began working with other journalists who had access to the Snowden documents. But because of the British government's actions, I had to leave the country in order to research the documents and write stories about what I found. I spent more than a year working in Brazil and the United States because they were safer environments. And when I returned to London I had to have lawyers waiting for me because they feared I might be arrested. Thankfully I was not. But the fact that it was even a consideration says something about the environment in which British investigative journalists work.

London's Metropolitan Police launched a criminal investigation into the Snowden revelations, because included in the trove there were documents about secret British surveillance programs. That investigation – named Operation Curable – is still active today, nearly five years on. The former head of the investigation, Cressida Dick, has said that one element of the investigation is focused on whether journalists who handled the classified documents violated the Terrorism Act, which contains a provision that makes it illegal to "elicit, publish or communicate" information about members of the intelligence services. There is a punishment of up to 10 years in prison for that offence.

As one of the world's oldest democracies, the UK should never feel like a hostile place for journalists. But sometimes, for me and others I have worked with, it does. There are many countries in the world where conditions are far worse for reporters, where you could be killed or tortured simply

55 Turvill, W. (2015): Interception Commissioner: 82 journalists' phone records grabbed by police in three years, judicial oversight needed, Pressgazette, 4 Feb. https://www.pressgazette.co.uk/interception-commissioner-82-journalists-phone-records-targeted-police-three-years-forces-should/

for publishing information. We are a far cry away from that here. But our country can and should be doing more to protect and defend press freedom. Journalists and their sources should never be spied on and investigated for producing news reports in the public interest.

Legal Professional Privilege in jeopardy

Ben Jaffey QC

Ben Jaffey QC is a barrister at Blackstone Chambers. He has appeared in most of the post-Snowden Investigatory Powers Tribunal claims, including Belhaj and Al-Saadi, the first successful claim against the security and intelligence services.

A lawyer needs to be able to have a private conversation with a client. This is the purpose of legal professional privilege. Privilege doesn't exist to protect lawyers or clients. It exists to make the justice system work. If a lawyer cannot be confident his or her advice is confidential, it will not be full and frank. Many clients won't be truthful with the lawyer unless the conversation is confidential.

"A lawyer needs to be able to have a private conversation with a client. This is the purpose of legal professional privilege. Privilege doesn't exist to protect lawyers or clients. It exists to make the justice system work."

I confess a personal interest. I represented two Libyan families who were subject to 'extraordinary rendition' back to Gaddafi's Libya in what seems to have been a joint operation between MI6, CIA and Libyan intelligence service.

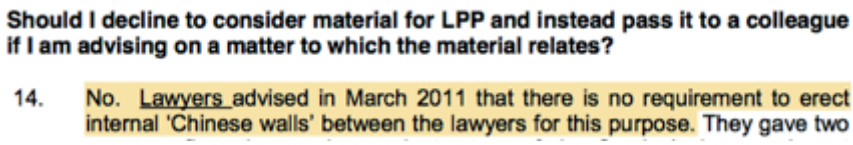
After the revolution, they brought tort claims in the UK. Some of my clients were senior members of the Libyan Islamic Fighting Group, a proscribed organisation. No-one would doubt they were under surveillance.

But they were also suing the UK Intelligence Services. So how is their right to legal privilege to be protected when under surveillance by the people they are suing? How can I, as their lawyer, have a confidential conversation about tactics, about a settlement, when the other side may be listening?

To find out, my clients brought a claim in the Investigatory Powers Tribunal. They sought disclosure of internal, previously secret policies about spying on privileged legal communications. I expected the policies would be pretty sound. There would be information barriers everywhere and strict secrecy rules.

To find out, my clients brought a claim in the Investigatory Powers Tribunal. They sought disclosure of internal, previously secret policies about spying on privileged legal communications. I expected the policies would be pretty sound. There would be information barriers everywhere and strict secrecy rules.

Sadly not. Here is MI5's previously secret policy on Legal Professional Privilege (LPP), written in a helpful Q&A format:



Should I decline to consider material for LPP and instead pass it to a colleague if I am advising on a matter to which the material relates?

14. No. Lawyers advised in March 2011 that there is no requirement to erect internal 'Chinese walls' between the lawyers for this purpose. They gave two

So if you are an MI5 lawyer and you see the other side's privileged legal advice in a case you are advising on, you can go right ahead and read it. I confess to some surprise that any lawyer could ever have advised this policy was lawful and that no-one blew the whistle on this. Not reading the other side's legal advice is week 1 of professional ethics at law school. Even worse, this policy was apparently signed off by the Intelligence Services Commissioner.

Eventually the case was conceded. The Government recognised that its policies were indefensible. New information barriers have been put in place. The Tribunal published a judgment saying that GCHQ had kept two of my client's privileged documents. The documents were destroyed. The Codes of Practice and the legislation were changed. But even under the new rules in the Investigatory Powers Act, privileged material is still fair game in a national security case. Under s. 27 of the Investigatory Powers Act 2016, legal professional privilege is reduced to a factor to be weighed against the public interest in obtaining the information, so long as there is no other way of obtaining it.

So when my clients in national security cases ask me "can I speak to you confidentially", my answer is still "no".

Vulnerable Groups and the State

Schools and surveillance: who is watching the watchers?

Jen Persson, defenddigitalme

Jen Persson founded defenddigitalme in 2015, as a non-profit, data privacy and digital rights group led by parents and teachers with the aim of making all children's data safe, fair, and transparent across the education sector in England.

Children in schools and young adults at universities are subject to state and commercial surveillance perhaps more than any other community in England. Visible surveillance tools like CCTV in playgrounds, corridors and private spaces such as bathrooms[56] or highly invasive all-seeing classroom cameras[57] are on the rise.

In addition, biometric systems are increasingly found in educational spaces. From handprint entry readers in an Oxford nursery, to fingerprints taken for cashless catering, tracking of library book loans, and access to lockers and printers in the majority of secondary schools, children are expected to hand over their sensitive biometrics from as early as age two. Thus, basic services like free school meals or libraries, can become inaccessible unless they agree to this intrusion. Biometric systems are mainly installed with the intention to ease administrative burdens and to save back office costs, when in reality, there is qualitative evidence[58] that these measures fail to materialise or simply displace tangible costs.

While these surveillance methods are noticeable, it is the collection of children's data that creates hidden surveillance far beyond the circle of people a child or their parents might expect. The cost for individuals is not only a threat to their lifetime privacy but a chilling effect on participation, others' perceptions of their potential, harm to young people's trust in confiding in an authority figure, and expectations of a professional duty of confidence.

56 BBC (2017) Kingswinford parents brand school toilet cameras 'creepy' https://www.bbc.com/news/uk-england-birmingham-41838556
57 Aston University Engineering Academy install Onvu (2018) http://defenddigitalme.com/wp-content/uploads/2018/07/camera_weston0.jpg
58 Leaton Gray, S. and Phippen, A. ,(2017): Invisibly Blighted, The Digital Erosion of Childhood,

Unseen surveillance through data

There are several ways in which the current education system gathers sensitive information about young people. For one, state school administrative databases in England focus primarily on delivering a way to benchmark local organisations within the state so that national comparisons can be made over time, and across the sector. In the process, each stage of a child's education is passed up the chain via a 'Common Transfer File'[59] to the next organisation. The Department for Education (DfE) demands a huge volume of data about individual children from state funded schools and nurseries, three times every year in the School Census, and other annual surveys.

Schools' internal information management systems predominantly managed by Capita SIMS in England, record a child's name, date-of-birth, ethnicity, gender, and family address, as well as[60] their behaviour and sensitive reasons for leaving the mainstream system for Alternative Provision, such as pregnancy or mental health. Special educational needs are also included in the national census.

This trove of sensitive data is increasingly used to link school records with other third-party datasets. Local authorities are joining educational data with information about individuals and households bought from data brokers like Mosaic or Acorn, to explore the possibilities of making early interventions based on algorithmically predicted behaviour. Researchers are also using national pupil data for predictive modelling to design classroom interventions based on children with a 'certain' profile.[61] Research teams at the Ministry of Justice are now using sensitive school data, such as information about children in care, to fill in the gaps on criminal databases such as provided by the Police National Computer,[62] and identify absent fathers in the family justice system.

However, this linking of records creates new risks. Reasons-for-exclusion labels from mainstream schooling can be interpretative and opinion based, but are widely shared in research, copied, distributed and treated for many years as facts on children's records. The children themselves and their families have no idea who knows what about them.[63] This usage could have unintended consequences for communities, when models based on predefined comparative and collective characteristics target a group of people, particularly when no data accuracy checks are made.

---

59 CTF 18 specification, version 1.0 (2018)
http://defenddigitalme.com/wp-content/uploads/2018/04/CTF_18_technical_specification_v_1_0.pdf
60 The Department for Education (2013): Common Basic Data Set. Available at: https://www.gov.uk/government/publications/common-basic-data-set-cbds-database
61 Case study: Institute of Criminology. Available at:
http://defenddigitalme.com/wp-content/uploads/2018/04/Cambs_Crimi_NPD.pdf
62 Case study: PNC and NPD data linkage. Available at:
http://defenddigitalme.com/wp-content/uploads/2018/04/PNC_NPD.pdf
63 The State Of Data2018 survey: Survation poll of parents of children age 5-18 in state education carried out for defenddigitalme on use of pupil data in England http://survation.com/wp-content/uploads/2018/03/Defend-Digital-Me-Final-Tables.pdf

Like the example of the Troubled Families Programme[64] shows, where families only have to match 2 criteria to be considered 'troubled', interventions are decided on a national level, even if carried out locally. Thus, surveillance through data can have effects with a permanency and authority that paper records previously did not have.

'Dataveillance' also stretches from schooling into higher education. Extensive data from Virtual Learning environments are combined with student enrolment data,[65] to profile and predict behaviours and outcomes. Complaints from staff and students made to defenddigitalme have included concerns about the breadth of data available to a wide range of staff, creating the risk of profiling and screening by ethnicity, religion, student and/or parental wealth which could have adverse effects on the treatment of students by staff, even if the intention was to be beneficial.

Commercial surveillance has become commonplace

The issue of dataveillance and sharing of sensitive data is not limited to public services and governmental institutions. As the volume of data about individuals has grown, companies that facilitate the gathering of data are eager to share it with third parties since data brokerage has become the primary business model for many.

Free-to-school apps are a pathway into pupils' data and parental purchasing power. Too often schools assume parents will want to use these products and pass on personal data by registering every child and their family without asking. If a parent later objects to the initial sign up, it is often too late to prevent a private company from having rights to access and use the data. Parents and children have no idea how many apps and third parties track and profile their use of software inside or outside the classroom.

Most of the time, parents and primary aged pupils do not even have a choice whether or not to use these systems when the school makes purchasing decisions. Some become central to a teacher's distribution of classroom materials, homework tracking and day-to-day activity, often without any school-level oversight.

The lack of knowledge and training around rights and responsibilities leaves a large gap for individual commercial exploitation through the introduction of new systems. Children are profiled, tracked online, targeted by advertising, and their data used to develop products and ultimately increase profit margins, all without any digital understanding or awareness. Some of the information gathered is very sensitive as children can post their photographs or hobbies into profiles which are all available to external viewers.

---

64 https://www.gov.uk/government/news/troubled-families-programme-annual-report-published
65 FOI request Edinburgh University, (2017) available at: https://www.whatdotheyknow.com/request/442554/response/1088273/attach/3/ResponseWithEnclosures.pdf

Surveillance under the guise of safeguarding in schools

Children and young people should not find that software introduced for their safeguarding, causes them lifelong reputational risk and real harm. Yet this is the result for some children wrongly labelled as at risk of suicide or gang membership, and whose details are passed on to third-parties including the police, under the Prevent duty.[66]

> ***Children and young people should not find that software introduced for their safeguarding, causes them lifelong reputational risk and real harm.***

Under the guise of safeguarding, surveillance software on children's school and home computers monitors what they do 24/7 every day of the year. Every keystroke is monitored and some software checks against libraries of over 20,000 watchwords. Every screen is captured. Some providers even permit the IT admin to operate a child's web camera[67] remotely and out of school hours when it is logged in to their school administered account for homework or when the child uses the laptop on the weekend or holidays. Impero's system even includes the word "biscuit" which they say is a term to define a gun.[68] This potentially affects more than "half a million students and staff in the UK".[69] Currently there is no understanding or oversight of the accuracy of this kind of software and instead of implementing accountability, black-box decision-making is often trusted without openness to human question.

Error rates are opaque and system providers have little incentive to be transparent. Teachers concerned enough to contact us said they have children who search for something uncontroversial, the system flags it, and only allows the staff to make a 'note', that it was an error, but not delete the error. Companies have no incentive to lower their "success rate" of events captured.

In our research of over 400 schools in England, we are yet to find one policy that makes any mention of the supplier name, or what policy there is on profiling, keywords of third party access, retention, error rate, or course of redress. 84% of parents in the State of Data survey said they believe they should be informed which keywords get flagged, and 86% want to know

66 Prevent duty for England and Wales. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/445977/3799_Revised_Prevent_Duty_Guidance__England_Wales_V2-Interactive.pdf
67 NetSupport NDA https://www.netsupportdna.com/education/safeguarding.asp#webcam-enabled
68 Impero (2016): Impero software's keyword library for US schools addresses online safety concerns such as self-harm and radicalization, 22 June. Available at: https://www.imperosoftware.com/us/resources/press-releases/impero-softwares-keyword-library-us-schools-addresses-online-safety-concerns-self-harm-radicalization/
69 Hansard, 11 October 2016, Communications Committee http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/communications-committee/children-and-the-internet/oral/41158.html

what the consequences are – but do not currently know.[70] The solution to many concerns about child safety, like self-harm or inappropriate content, are human and not one-size fits all technologies.

Social Media as a Surveillance Tool

Laws and regulations have been left behind, as monitoring young people's social media in school and universities has become a common practice. Thus, protecting a young person's social media from unwanted monitoring is very difficult.

The Student Loans Company has been accused in the summer of 2018 of accessing content students post on social media pages that are not restricted to private (such as an open Twitter feed) to identify fraudulent applications for funds available to those without family support.[71]

Concerned parents have also contacted us about their own social media feeds being monitored when they found out that schools added photos of their teen at an anti-fracking demonstration, outside school hours, to the child's school record. The chilling impact this surveillance has on students' and parents' free speech, willingness to ask questions, and criticism is often embedded in school-home policy agreements, in which both parents and children are required to sign that they will not cause the school reputational harm.

Where do we go from here?

According to the Department for Education new technology is set to spearhead a classroom revolution.[72] While the Secretary of State, Damian Hinds, believes only a minority of schools and colleges are currently taking advantage of these opportunities, both schools and the DfE are taking too little note of the risks and harm, and how to mitigate them. Children's human rights to a full and free development, as established in the UN Convention on the Rights of the Child,[73] are under unprecedented threat in England today.

We can already start to see the dangers and harms to individuals and groups resulting from errors and bias in the data that feeds into the Prevent programme, and the exposure to exploitation risks. However, the long term impact of amassing children's data today and the chilling effects of classroom surveillance may be yet to be felt, since the impacts are under-researched.[74]

70 Defenddigitalme (2018): Only half of parents think they have enough control of their child's digital footprint in school. Available at: https://defenddigitalme.com/2018/03/only-half-of-parents-think-they-have-enough-control-of-their-childs-digital-footprint-in-school/
71 The Guardian, 8 August 2018, https://www.theguardian.com/education/2018/aug/08/student-loans-company-reviews-processes-after-spying-scandal
72 Education Secretary challenges the tech industry to launch an education revolution for schools, colleges and universities. August 2018. Available at: https://www.gov.uk/government/news/new-technology-to-spearhead-classroom-revolution
73 Unicef. UN convention on the Rights of the Child. Available at: https://www.unicef.org/crc/index_30177.html
74 Leaton Gray, S. and Phippen, A. (2017): Invisibly Blighted - The Digital Erosion of Childhood, p.92.

Political agendas change. Children's Schools Census data has already been misused to identify undocumented migrant children and their family members. The UK has effectively registered all Roma families through their children's school records – what if a future government decided on a Roma policy as discussed in Italy in the summer of 2018?[75]

If a child is an undocumented migrant, an ethnic minority, a non-conformist, or simply not liked by staff, some of the current school software and surveillance systems are more likely to pick them out for intervention than their classmates. Systemic unfairness encoded into data and algorithms, is given an authority it does not deserve. Data can be badly understood and result in harmful false predictions and mistaken conclusions. Children are, by default, being disempowered from understanding or correcting decisions and predictions made about them.

Profiling children by their search terms through web monitoring including remote camera access to children's devices during and beyond school hours should be urgently reviewed, as we set out in our State of Data 2018 report.[76] It should be of utmost priority that teachers and all educational staff are trained in digital literacy, data protection and privacy rights. Oversight and accountability, for both human and algorithmic usage of education data, need urgent regulatory attention. Children and young people must be given a better digital understanding of their own data, if our future society is to flourish.

75 Kirchgaessner, Stephanie (2018): Far-right Italy minister vows 'action' to expel thousands of Roma, The Guardian, June 19. Available at: https://www.theguardian.com/world/2018/jun/19/italy-coalition-rift-roma-register-matteo-salvini

76 defenddigitalme (2018): The State of Data 2018, (p22). Available at: http://defenddigitalme.com/wp-content/uploads/2018/05/StateOfDataReport_policymakers_ddm_sml.pdf

Turning frontline workers into border guards: data-sharing and immigration enforcement

Gracie Bradley, Liberty

Gracie Bradley is an activist, writer, and Policy & Campaigns Manager at Liberty. She has wide-ranging expertise in human rights and immigration, data protection, counter-terror and policing. Before joining Liberty, Gracie worked in casework, research and policy across several NGOs to support survivors of torture and working migrants to secure their rights while navigating the UK's immigration system.

Liberty (the National Council for Civil Liberties) is one of the UK's leading civil liberties and human rights organisations. Liberty works to promote human rights and protect civil liberties through a combination of test case litigation, lobbying, campaigning and research.

Introduction: the hostile environment

Since 2012, the Government has operated with an explicit commitment to create a "hostile environment" for undocumented migrants.[77] In 2012, then Home Secretary Theresa May said:

> "The aim is to create here in Britain a really hostile environment for illegal migration. Work is under way to deny illegal immigrants access to work, housing and services, even bank accounts. What we don't want is a situation where people think that they can come here and overstay because they're able to access everything they need."[78]

77 Undocumented migrants are people in the UK who need permission to enter or remain in the country, but who do not have it. This could include, for example, a person who came into the country on a valid visa, but was unable to renew it; or a person who came to the UK and claimed asylum, but had their application refused, and has no further right to appeal.

78 Theresa May interview: 'We're going to give illegal migrants a really hostile reception', The Telegraph, May 2012: https://www.telegraph.co.uk/news/uknews/immigration/9291483/Theresa-May-interview-Were-going-to-give-illegal-migrants-a-really-hostile-reception.html

First and foremost, hostile environment policies function to deny undocumented migrants access to essential goods and services, like free healthcare, lawful work, rented accommodation and bank accounts.[79]

They turn frontline workers into border guards and Home Office informants, requiring them to check the immigration status of people trying to access those goods and services and using the data they collect for immigration enforcement purposes.

These public servants are transformed – often unwillingly and unknowingly – into spies, made to serve their part in a system of targeted surveillance designed to monitor undocumented migrants' every interaction with essential frontline services.

Even seriously ill people and children are seen as fair game by the Government in its determination to aid deportations at any human cost.

And, in order for undocumented migrants to be denied access to goods and services, we all end up having to show photo ID to do things as mundane as registering with a GP or renting a flat.

At the same time, the Government has cut access to legal aid and appeal rights, raised fees for immigration and nationality applications and changed the already complicated immigration rules repeatedly.

All of this means people are more and more likely to become undocumented, even if they did not intend to break the immigration rules.

Shadowy data-sharing practices

Several hidden data-sharing schemes have been exposed since the hostile environment came into force.

The Home Office, Department of Health and Social Care and NHS Digital had an agreement allowing the Home Office to use confidential medical records to obtain the addresses of patients suspected of being undocumented.[80] The Government suspended that agreement in May 2018 following a campaign by civil society and politicians.[81] It has promised to publish a new version, which it says will restrict data-sharing to cases involving "serious crime" – although it has yet to explain what exactly this means in practice.[82]

The Home Office and Department for Education have also had an agreement since at least 2015, letting the Home Office use confidential school records

---

79 For more information about the hostile environment, see 'A Guide to the Hostile Environment', Liberty et. al., April 2018: https://www.libertyhumanrights.org.uk/sites/default/files/HE%20web.pdf

80 'Memorandum of Understanding between Health and Social Care Information Centre and the Home Office and the Department of Health', 27 September 2016: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/585928/MOU_v3.pdf

81 They are still sharing data where there is a "clear demonstrable risk to public safety or risk to the individual themselves".

82 NHS Digital, Memorandum of Understanding Revision Plan, June 2018: https://digital.nhs.uk/services/national-back-office-for-the-personal-demographics-service/memorandum-of-understanding-revision-plan

to obtain the addresses of children and their family members who it suspects of being undocumented.[83]

Over half of UK police forces routinely refer undocumented victims of crime to the Home Office.[84]

> ***In general, people are not told when interacting with frontline services that their personal information may be shared with the Home Office for immigration enforcement purposes. Many workers, such as receptionists, doctors and teachers, are unaware that this web of surveillance exists – and the same goes for the wider public.***

The Greater London Authority has also used information collected by homelessness outreach workers to assist the Home Office in its deportations of migrant rough sleepers.[85]

More broadly, agreements operate between the Home Office and various agencies to ensure undocumented migrants cannot access bank accounts, driving licences,[87] work or welfare benefits.[88] The Government has paused some of these in the wake of the Windrush scandal – but only temporarily and, even then, only in relation to people aged over 30.[89]

In general, people are not told when interacting with frontline services that their personal information may be shared with the Home Office for immigration enforcement purposes. Many workers, such as receptionists, doctors and teachers, are unaware that this web of surveillance exists – and the same goes for the wider public.

Most agreements have been unearthed through Freedom of Information Act requests – and Parliament has scarcely debated their human rights implications.

85 Agreement obtained through FOIA by Liberty and reported by The Observer, 'Home Office used charity data map to deport rough sleepers', 19 August 2017: https://www.theguardian.com/uk-news/2017/aug/19/home-office-secret-emails-data-homeless-eu-nationals
86 Cifas is a third sector organisation that holds the UK's largest anti-fraud database. A data-sharing agreement between it and the Home Office is referenced at paragraph 2.6 in Independent Chief Inspector of Borders and Immigration (ICIBI), 'An inspection of the 'hostile environment' measures relating to driving licences and bank accounts', October 2016: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567652/ICIBI-hostile-environment-driving-licences-and-bank-accounts-January-to-July-2016.pdf
87 ICIBI, ibid.
88 Agreements obtained by Liberty and journalists through FOI requests, and referenced in Vice Magazine, 'Theresa May's 'Anti-Slavery' Agenda Is About Deporting Migrants', 21 September 2017: https://www.vice.com/en_uk/article/8x8qbv/theresa-mays-anti-slavery-agenda-is-about-deporting-migrants
89 'UK government pauses hostile immigration policies after Windrush', The Guardian, 11 July 2018: https://www.theguardian.com/uk-news/2018/jul/11/windrush-uk-government-pauses-hostile-immigration-policies

What these practices mean for undocumented migrants and wider society

Secret data-sharing for immigration enforcement purposes is a form of targeted surveillance that subjects undocumented migrants to intrusive monitoring – and enlists trusted public servants to monitor them.

It is an invasion of privacy, harmful not only to undocumented migrants, but to society as a whole. If people know that seeking support from their doctor, their child's school or the police may lead to their deportation, they are highly likely to be deterred from doing so.

This undermines important public policy aims such as protecting public health, child safeguarding and the prevention of crime.

Secret data-sharing destroys trust between frontline workers and people interacting with essential services. It also sets a precedent that undermines the privacy of every one of us – that once we share our personal data for one purpose with a frontline service, the Government can use it for any other purpose without our knowledge or consent.

Health

Home Office use of patient data for immigration enforcement purposes drastically undermines doctor-patient confidentiality – the cornerstone of our NHS.

This data-sharing also interacts with other barriers to healthcare – such as charging fees for treatment to discourage people from accessing care.

People may avoid seeking medical help until they are seriously ill, rather than attending as soon as they notice symptoms. For those who are pregnant or have progressive illnesses, a delay can be costly, dangerous and potentially fatal.

In one known case, a domestic worker died after refusing to seek help for an undiagnosed disease due to fear that she would be reported to immigration services.[90] This woman was also violently abused by her employer and, in one instance, scalded with hot water. She did not report her injuries or the incident as she was too afraid to alert the authorities.

90 Voice of Domestic Workers, Health Select Committee, Oral Evidence: Memorandum of understanding on data-sharing between NHS Digital and the Home Office, HC 677, 16 January 2019, http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/health-and-social-care-committee/memorandum-of-understanding-on-datasharing-between-nhs-digital-and-the-home-office/oral/77354.html

Ultimately, the abuse was not what killed her – it was the fact that her disease went untreated because she was too frightened to seek help.

Policing

There have been many reports of harrowing incidents stemming from police data-sharing and the hostile environment.

In 2017, a woman who was five months pregnant reported to police that she had been repeatedly raped – but was subsequently arrested at a rape crisis centre on immigration grounds.[91]

In another case, a man who reported an assault to police ended up in immigration detention himself.[92]

The Government must prioritise preventing and investigating serious and violent crime over taking enforcement action against undocumented migrants. If undocumented migrants cannot report crimes to police without fear of deportation, people seeking to injure, exploit or otherwise harm them will be emboldened to do so with impunity – making all of us less safe.

Education

Secretly using children's school records to deport them and their family members can only undermine any attempt to create inclusive educational environments for children, as many teachers and local authorities strive to do.

At best, it undermines trust between children, parents and teachers, encouraging teachers to view migrant pupils as objects of suspicion.

At worst, it risks leading to children of undocumented migrants being removed from school due to fear of immigration enforcement, exacerbating the already significant barriers to health and development that they and their families already face – and potentially meaning that they miss out on education entirely.

---

91 Politics.co.uk, Woman reports rape to police - and is arrested on immigration charges, 28 November 2017 http://www.politics.co.uk/news/2017/11/28/woman-reports-rape-to-police-and-is-arrested-on-immigration; Politics.co.uk, Met police hands victims of crime over to the Home Office for immigration enforcement, 5 April 2017: http://www.politics.co.uk/news/2017/04/05/met-police-hands-victims-of-crime-over-to-the-home-office
92 See: https://twitter.com/BIDdetention/status/1002115789158256640

The solution: a firewall

The Government should implement a firewall – a promise that data will not be shared between Home Office immigration control and other departments. Independent, indiscriminate public services underpin every person's ability to enjoy their human rights and lead a dignified life. These data-sharing agreements undermine that. They are a dangerous step towards a general principle that the Government may repurpose data collected by any trusted service, without our consent, to meet another public policy aim.

Creating an atmosphere of hostility and fear damages people's trust in public services. This is particularly concerning for the NHS, whose main role is to provide high-quality, safe and confidential care to all patients – regardless of their background, origin or residency status.

It is particularly concerning in education, the primary function of which is to provide children with high-quality teaching in a safe environment, without discrimination.

The broader risks these practices pose to our privacy are also alarming. By prioritising immigration enforcement over the protection of essential public service data, and co-opting frontline workers into the surveillance of undocumented migrants, the Government is endangering our human rights, important public policy aims and the future confidentiality of our public services.

These crucial objectives will be jeopardised further – unless the Government creates an iron-clad firewall to stop this toxic data-sharing for good.

Monitoring, Suspicion and Welfare

Dr Jay Watts, Consultant Clinical Psychologist

Dr Jay Watts is a consultant clinical psychologist and psychotherapist who has been working in mental health for 20 years. She is also an activist who runs a clinic for those on long-term disability benefits as part of a wider endeavour to make long-term psychotherapy available for all.

Since 2012, unprecedented new techniques of sanction, surveillance and deterrence have had a profound and devastating effect on the mental and physical health, and life expectancy, of benefits claimants.[93] The situation is now so dire that it is nothing less than a human rights emergency with stress, fear, guilt and anxiety provoked by this climate shift a key trigger in many deaths by suicide.[94] It is, in the words of the Chair of the United Nation's Committee on the Rights of Persons with Disabilities, a "human catastrophe" that is happening here and now in the UK.[95]

Let me start with an example:

Gerry[96] is a fifty something man with a diagnosis of severe depression that has resulted in multiple hospital admissions. Gerry suffered chronic and repeated traumas and displacement in his childhood that was so severe that his ongoing survival is a real achievement. Gerry has always served the community, not as a taxpayer - he is not well enough to work - but by leading community groups at the local hall where people who do not feel safe enough to engage with psychiatric services could find their voice, some warmth, and a bit of compassion.

93 Fletcher, D. R., & Wright, S. (2018). A hand up or a slap down? Criminalising benefit claimants in Britain via strategies of surveillance, sanctions and deterrence. Critical Social Policy, 38(2), 323-344.
94 Bulman, M. (2017). Attempted suicides by disability benefit claimants more than double after introduction of fit-to-work assessment. The Independent, 28th December. Available at: https://www.independent.co.uk/news/uk/home-news/disability-benefit-claimants-attempted-suicides-fit-to-work-assessment-i-daniel-blake-job-centre-dwp-a8119286.html [Accessed 9 Aug. 2018].
95 Kentish, B (2017). Government cuts have caused 'human catastrophe' for disabled, UN committee says. The Independent, 25th August. Available at: https://www.independent.co.uk/news/uk/politics/government-spending-cuts-human-catastrophe-un-committee-rights-persons-with-disabilities-disabled-a7911556.html [Accessed 25 Aug. 2017].
96 Gerry has given me permission to write this vignette, in the interest of gaining public awareness. Various details have been changed to preserve anonymity

When the changes to benefits kicked in,[97] state suspicion and monitoring of claimants soon increased. Gerry was faced with constant questions from the Department for Work and Pensions (DWP) about why he was able to volunteer and not work. They started to insist that Gerry go to courses on 'positive psychology' so he could be 'work-ready', and he was threatened with sanctions if he failed to oblige. Gerry tried to explain what all mental health practitioners know - that it is a wildly different thing to do voluntary work where one can come and go according to the vicissitudes of mental health without pressure as opposed to paid work.

Unable to persuade the DWP, and experiencing constant thoughts that he was 'worthless' for being workless, Gerry fell into a depression far deeper than he had experienced in recent decades. He became agoraphobic - unable to leave his flat - for the first time ever and the community group that had meant so much to so many people, and provided such a strong sense of identity and value to Gerry, fell apart. So too did Gerry's capacity to care for himself and he stopped eating and cleaning himself properly. When a neighbour eventually checked in on Gerry - where was he? - she found piles of letters unopened from the job centre letting him know his benefits had been stopped. Gerry was still alive, just, but in the worst physical and mental health he had been in for decades. Gerry was sectioned under the Mental Health Act for his own safety. As is so often the case nowadays, his mental health team directly connected his deterioration with his experiences in the new, radically altered welfare state.

> ***The spectre of surveillance as a deterrence technique instills anxiety and leads of internalised moral suspicion in claimants whose thoughts become dominated by the idea that they have done or might do something wrong***

Until a few years ago, if a patient with a diagnosis of paranoid schizophrenia told you that they were being watched by the DWP, most mental health practitioners would presume this to be a sign of illness. This is not the case today.

The level of scrutiny all benefits claimants feel under is brutal. Even Sainsbury's now has a policy to share CCTV "where we are asked to do so by a public or regulatory authority such as the police or the Department for Work and Pensions".[98] Gym memberships, airport footage, job centres and surveillance video from public buildings are now used to build cases against claimants, with posts from social media used to suggest people are lying about their disabilities. The environment is paranoid and controlling,

97 Mills, T. (2018): PIP: New benefits system 'demeaning and degrading', The BBC, 1 May. Available at: https://www.bbc.co.uk/news/uk-northern-ireland-43968546

98 Watts, J. (2018). No wonder people on benefits live in fear. Supermarkets spy on them now. The Guardian, 31st May. Available at: https://www.theguardian.com/commentisfree/2018/may/31/benefits-claimants-fear-supermarkets-spy-poor-disabled. [Accessed 9 Aug. 2018].

fuelled by pervasive suspicion. There is little escape from this environment for claimants, as speaking freely on social media has become increasingly dangerous.

There are countless examples of surveillance teams mounting operations against claimants, in many cases as a result of a disgruntled neighbour or former partner calling, anonymously, the National Benefits Fraud Helpline. Surveillance tactics include following and recording people, for example by placing hidden cameras in a bottle of Coca-Cola in a place a claimant frequents.[99] The state can use such intrusive surveillance for a reported 'breach' as minor as a single parent living with someone and received an extra £6 for not reporting this[100] (often without realising they are supposed to do this). Frequent 'Compliance Officer' checks perpetuate this environment of suspicion all claimants now live in. These checks can occur randomly or after a tip-off but are common enough to be a new norm locking bodies and minds into a dangerous state of constant threat-alert. Almost 4,000 people are employed by DWP to investigate benefit fraud, despite official estimates evaluating that only 0.7% of claims may be fraudulent.[101] Nearly everyone that I come across on benefits now lives in a climate of such fear as a result of this combination of visibility, scrutiny and sanctions that life often seems unbearable.

The spectre of surveillance as a deterrence technique instills anxiety and leads to internalised moral suspicion in claimants whose thoughts become dominated by the idea that they have done or might do something wrong. This is the case, in my experience, for almost all claimants - not just for the miniscule few committing fraud, and not just among the thousands with pre-existing mental health problems.

An argument popularised in the wider surveillance debate has had leverage here too: if claimants have nothing to hide, surely they have nothing to fear? The DWP argues video and social media footage is only used in extreme circumstances. However, this argument is not only depoliticised and detached from basic rights principles – it ignores a key psychological truth. One does not need to have done anything wrong to feel that one has done something wrong. Why do we feel anxious going through security at airports? Why do we feel the need to 'perform' innocence? Those feelings are just a fraction of what many claimants experience, 24 hours a day, seven days a week, intruding into their home and social life in an all pervasive, unprecedented way.

To make sense of this, it can be useful to think of the metaphor of the Panopticon.[102] Jeremy Bentham designed the Panopticon in the eighteenth century as an institutional building with a tower surrounded by cells which

99 Gentleman, A. (2011). Benefit fraud: Spies in the welfare war. The Guardian, November 1st. Available at: https://www.theguardian.com/society/2011/feb/01/benefits-fraud-investigators. [Accessed 13 Aug. 2018].
100 Is there a policy doc or law JW can share with us so we can verify this kind of surveillance can be used in these cases please?
101 Garside, J. (2016). Benefit fraud or tax evasion: row over the Tories' targets. The Guardian, 13th April. Available at: https://www.theguardian.com/uk-news/2016/apr/13/benefit-or-tax-evasion-row-over-the-tories-targets [Accessed 13 Aug. 2018].
102 Bentham, J. (1843). The Works of Jeremy Bentham (Vol. 7). W. Tait.

allowed a watchman to observe occupants - workers, prisoners or children - without them being aware if they were being watched or not. The shining light from the tower was so bright that people had to act as if they are always under observation, permanently exposed, isolated and paralysed under the gaze of potential judgment (for how could they know if there was a watchman there). The philosopher Michel Foucault took up this metaphor in Discipline and Punishment to describe how disciplinary power functions as people internalise the idea that they are being watched, monitoring their behaviours accordingly and shaping their sense of themselves.[103] This produces what Foucault called a compulsory visibility. "It is this fact of being constantly seen, of being able always to be seen" Foucault wrote, "that maintains the disciplined individual in his subjection".[104]

Claimants today live this subjection, this sense of visibility and targeted surveillance, with devastating effects on mental and physical health. They often feel unable to go out, attempt voluntary work or enjoy time with family and friends for fear this will be used as evidence against them. The atmosphere against claimants is so hateful, so degrading, so ill-informed about the vicissitudes of energy and ability core to mental and physical disabilities, that they become imprisoned in the home or in a mental state wherein they are constantly being accused of being fraudulent or worthless given our tendency as humans to internalise what others think of us. This is combined with a relentless pressure to demonstrate attempts to return to work. For example, DWP Work Coaches monitor claimants online activity meaning that claimants with even the most severe disabilities are unable to privilege their health needs, being required instead to constantly update their CV and apply for jobs even when medical evidence shows this is counterproductive to health.

I'll end with a testimony from the psychiatric survivor-led activist group Recovery in the Bin.

"The best way of describing DWP surveillance (and the wider 'scrounger rhetoric of government and media) and its effects is to say that claimants live in a parallel subculture to the society everyone else lives in. We live in something akin to the former East German Stasi regime. The fear, paranoia, and anxiety are disabling and have massively degraded many people's lives. Some have become virtual shut ins and recluses from fear of being seen 'doing something normal' and it being used against them. Family life and childcare have been damaged (being seen playing with your child is feared as it can be used against you), the government promote a hotline for people to report their neighbours. We do not have the protections of the criminal justice system or the human rights act in reality, we can be starved on the whim of DWP employees who have targets to achieve sanctions. Many have died and many are living far worse lives because of the atmosphere of pervasive surveillance and summary punishment".

103 Foucault, M. (1977). Discipline and Punish: The Birth of the Clinic. New York: Vintage.
104 Ibid., 189.

The government has abandoned any consideration of meeting human needs for an obsession with establishing a disciplined and regimented society where work or the pursuit of work is fetishised above all else, and wherein those who fail to pursue this ideal are, overtly, punished and, covertly, demonised.

Claimants do not need to turn on Netflix to experience a dystopian world today - it is fast becoming an everyday reality.

Activist organisations working in this space include Disabled People Against Cuts, Recovery in the Bin, Mental Health Resistance Network, Black Triangle and Boycott Welfare.

Conclusion

Surveillance has permeated almost every aspect of our lives. A future that, to many, may seem distant and unimaginably dystopian, is very much a reality in 2018. As the contributions to this report demonstrate, it does not matter if we have something to hide or not. In our mass surveillance society, anyone and everyone is under suspicion and observation, whether justified or not.

If we want to change this state, we need to be more alert to the subtle changes that threaten our civil liberties. The testimonies in this report are only the tip of the iceberg, and most surveillance happens without anyone ever finding out. But this silent erosion of our rights must be brought to a halt. Suspicionless surveillance not only affects the individual but skews our perception of others, and risks morphing our society into a repressive and authoritarian one where principles of free speech and expression are under-valued. Privacy is key in the delicate power balance between the citizen and the state.

After all, in what kind of society do we want to live?

We believe that a life without suspicionless surveillance, discrimination, oppression and unfair intrusion is possible. Big Brother Watch will continue to work with the groups represented in this report to make that vision a reality.

BIG BROTHER WATCH

DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

bigbrotherwatch.org.uk | @bbw1984