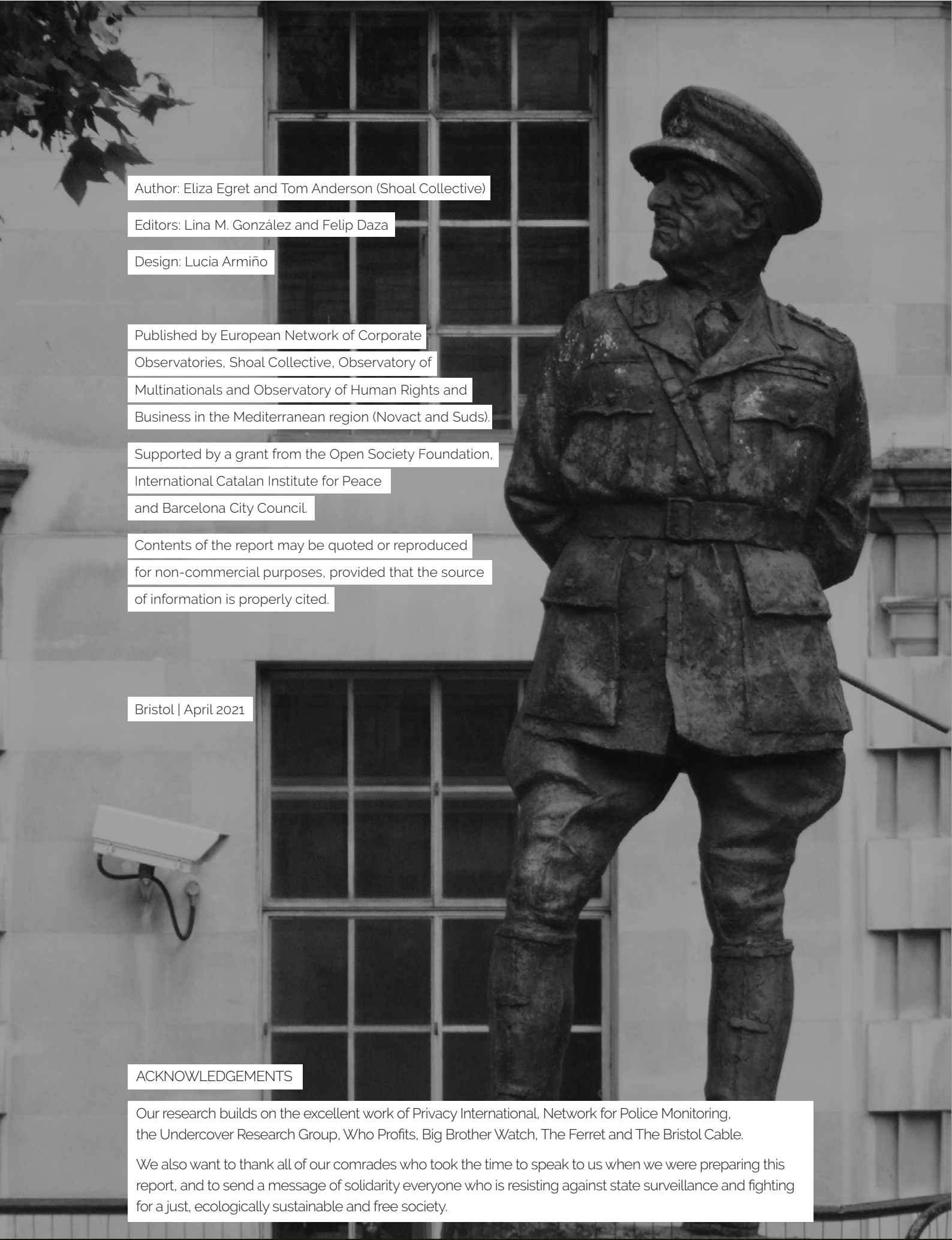
MASS SURVEILLANCE
AND CONTROL OF EUROPEAN DISSIDENCE

UK

The UK surveillance state

Building on centuries of colonial repression

ENCO EUROPEAN NETWORK OF CORPORATE OBSERVATORIES
Observatoire des Multinationales SOCIAL, ÉCOLOGIQUE, POLITIQUE
ODHE Observatori de Drets Humans i Empreses a la Mediterrània
shoal radical writing for a world beyond capitalism



Author: Eliza Egret and Tom Anderson (Shoal Collective)

Editors: Lina M. González and Felip Daza

Design: Lucía Armiño

Published by European Network of Corporate Observatories, Shoal Collective, Observatory of Multinationals and Observatory of Human Rights and Business in the Mediterranean region (Novact and Suds).

Supported by a grant from the Open Society Foundation, International Catalan Institute for Peace and Barcelona City Council.

Bristol | April 2021

ACKNOWLEDGEMENTS

Our research builds on the excellent work of Privacy International, Network for Police Monitoring, the Undercover Research Group, Who Profits, Big Brother Watch, The Ferret and The Bristol Cable.

We also want to thank all of our comrades who took the time to speak to us when we were preparing this report, and to send a message of solidarity everyone who is resisting against state surveillance and fighting for a just, ecologically sustainable and free society.

This report and the webdoc are part of the research, advocacy and education projects coordinated by Suds and Novact in collaboration with Shoal Collective and the Observatoire des Multinationales. The donors are not responsible for any use that may be made of the information it contains.

CONTENTS

METHODOLOGY

Some of the methods that we used to research this report were:

- Review of company, industry press and police websites, and the information made available by journalists, researchers and campaign groups.
- Freedom of Information (FOI) requests to police forces and local councils, and drawing on public FOI information via the WhatDoTheyKnow website.
- Search of the EU's Tender's Electronic Daily website.
- Search for contracts awarded by the police and government bodies through Gov.UK's Contracts Finder and the Bluelight Procurement Database.
- Interviews with campaigners, activists and other members of the public who are affected by the technology.
- Searches of Bureau Van Dyck's Orbis business information database.

INTRODUCTION

The UK has a reputation as a surveillance state, and with good reason: London has one CCTV camera for every 14 residents.[1] New surveillance technologies such as facial recognition and police drones are already a reality across the UK, with British legislation permitting more state surveillance of private communications than any other country in Europe.[2]

The UK is also one of the world's largest exporters of surveillance technology with British companies selling phone-hacking technology, spyware and facial recognition software overseas.[3]

However, surveillance is nothing new for the British state. It has a long history of espionage and surveillance, one that has been honed in its subjugation of colonised populations across the world for centuries. The proliferation of digital technologies, however, has created an environment where the UK surveillance state has been stepped up to new and deeply invasive levels, threatening our privacy and our freedom.

This report presents an overview of the use of different types of surveillance technology in the UK, as well as the companies providing the equipment. We also examine how this oppressive technology is being mobilised against social movements in the UK and how the effects of surveillance are being felt disproportionately by working class people and communities of colour.

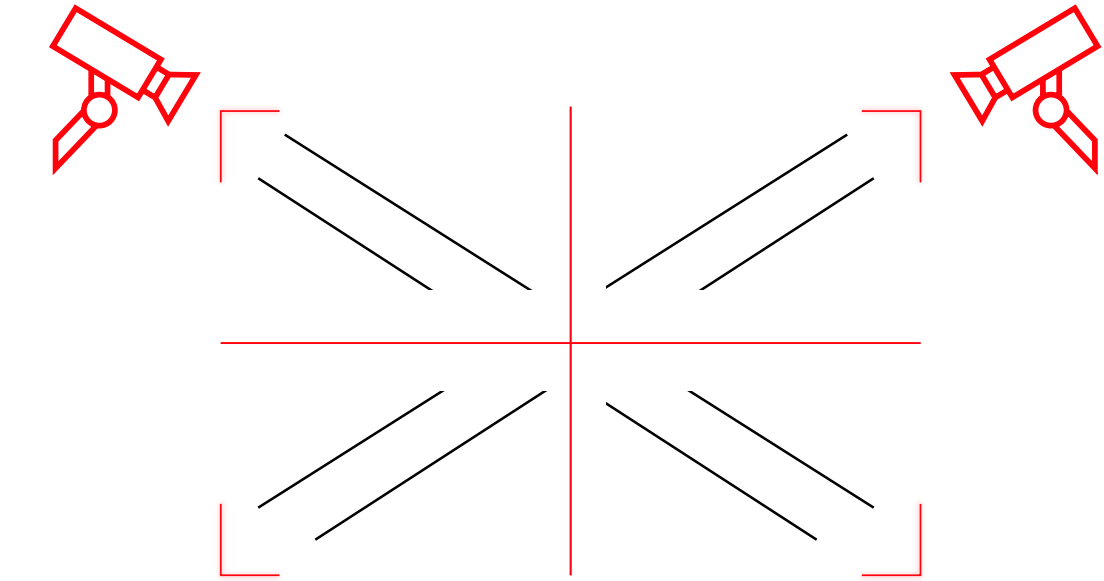
1 Keegan, M. August 14 2020, 'The most surveilled cities in the world', ***US News*** https://www.usnews.com/news/cities/articles/2020-08-14/the-top-10-most-surveilled-cities-in-the-world [Accessed March 16, 2021].

2 Griffin, A. November 2016, 'Britain just got perhaps the most intrusive spying powers ever seen' ***The Independent***. https://www.independent.co.uk/life-style/gadgets-and-tech/news/snoopers-charter-2-investigatory-powers-bill-parliament-lords-what-does-it-mean-a7423866.html [Accessed March 12, 2021].

3 Privacy International, July 2016, 'The Global Surveillance Industry' https://privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf [Accessed March 16, 2021].

The UK surveillance state: Building on centuries of colonial repression

1 SURVEILLANCE AND THE BRITISH STATE



The UK is becoming an increasingly high-tech surveillance society. But the use of surveillance by the British state is nothing new. As a colonial power, the British Empire relied heavily on state surveillance for many centuries to bring occupied peoples under its control and pacify them. What has changed in recent years is the range of repressive technologies which are being developed and rolled out by private companies and the increased reliance on digital technology, ushering in an era of state surveillance on steroids.

Similarly, in the past two decades the British government has pursued counter-terrorism policies and evoked a national security narrative that justifies the deployment of mass surveillance technologies under the pretext that such measures will keep us safe. Advances in technology, coupled with this national security narrative, have enabled the state to escalate its social control to unprecedented levels.

SURVEILLANCE AND COLONIALISM

Harvesting data about colonised populations has allowed the British state to monitor, control manipulate and divide communities, a central component of Britain's divide and conquer strategy. The data gathered has informed the repressive tactics deployed by the British state against colonised populations, to the benefit of the British Empire. It is beyond the scope of this report to delve deeply into Britain's dark colonial past, but here are some telling examples with regard to colonialism and surveillance.

Ireland, Britain's oldest colony, has served as a testing ground where British surveillance and control tactics were developed and refined for centuries before being implemented elsewhere. Following the Irish rebellion of 1798, the British state undertook mass surveillance of the Irish population, including the collection of statistics and census data.[4] Spies and informers who infiltrated the Irish republican movement at the time played an important role in compromising the 1798 rebellion, and subsequent attempts to overthrow British rule.[5] This monitoring enabled the British to control the Irish population more robustly, and to play nationalist and unionist populations off against each other.[6]

British colonialists in India in the 18th and 19th centuries systematically gathered data on the subjugated population for the purpose of taxation and social control. After the 1858 Indian rebellion against the British East India Company, efforts gathered apace to develop a new system of 'scientific' population classification in

4 McQuade, B. Neocleous, M. 2020, 'Beware: Medical Police', ***Radical Philosophy,*** https://www.radicalphilosophy.com/article/beware-medical-police. [Accessed March 12 2021].

5 *Óg Ó Ruairc, P. 2017,* 'Spies and informers beware!' ***History Ireland,*** https://www.historyireland.com/volume-25/issue-3-mayjune-2017/spies-informers-beware/ [Accessed March 12 2021].

6 Hadden, P. 1980, 'Divide and Rule (Introduction)', Marxists.org, https://www.marxists.org/history/etol/writers/hadden/1980/divrule/introduction.html [Accessed March 12 2021].

order to enable the famous British 'divide and rule' strategy, which consolidated British rule by weaponising the divisions between India's different religious communities and castes.[7]

Indeed, the technologies of the modern day surveillance society can be clearly seen to have colonial roots. According to Elia Zureik:

> *'It is significant that the basic tools of surveillance as we know them today (fingerprinting, census taking, map-making and profiling – including the forerunners of present day biometrics) were refined and implemented in colonial settings, notably by the Dutch in Southeast Asia, the French in Africa, and the British in India and North America.'*[8]

The British mandate rulers of Palestine built on the surveillance methods deployed in India. In the years following World War I the British introduced ID cards as part of their repression of the Arab Revolt of the 1930s, along with control systems such as security fences, watchtowers, permit systems and checkpoints.[9]

The UK's use of surveillance as a colonialist strategy has become increasingly high-tech in recent decades, mirroring the advances in surveillance technology more broadly. Since 2007, the British occupation of Afghanistan has utilised unpiloted aircraft, or drones. Similarly, drones have also been used by British troops in Iraq and Syria. The use of these high-tech aircraft means that whole populations spread across vast geographical areas can be kept under constant surveillance to an extent that would have previously been impossible. Moreover, fatal airstrikes can be carried out by remote control and from a distance without deploying occupying ground troops.[10] The use of high-tech surveillance technology by Britain as a tool in modern warfare is of grave concern, but a deeper discussion on this is beyond the remit of this paper.

7 Zureik, E. November 2013, 'Colonial Oversight', https://www.redpepper.org.uk/colonial-oversight/ [Accessed March 12 2021] and Tharoor, S. 2017, 'The Partition: The British game of 'divide and rule'', ***Al Jazeera,*** https://www.aljazeera.com/opinions/2017/8/10/the-partition-the-british-game-of-divide-and-rule/ [Accessed March 12 2021].

8 ***Ibid.***

9 ***Ibid.***

10 House of Commons Briefing Paper, October 2015, https://researchbriefings.files.parliament.uk/documents/SN06493/SN06493.pdf [Accessed March 12 2021].

CONSTRUCTING A SURVEILLANCE SOCIETY AT HOME

The surveillance and monitoring employed by the British colonialist state abroad has also informed the development of a domestic surveillance state at home. When populations have rebelled against, or have threatened to shake or topple the status quo, one of the state's responses has been to monitor them, in order to pre-empt and pacify any resistance. Nowhere has this been clearer than in how the British government has dealt with the north of Ireland, which is still under British rule.

The north of Ireland has seen a raft of British state surveillance tactics deployed, particularly against its nationalist population, since 1969. These tactics were part of a counter-insurgency strategy, which relied on undercover secret units, mass-screening and surveillance. These measures accompanied more aggressive tried and tested colonialist tactics such as internment (imprisonment without trial), military deployment in urban areas, military checkpoints, ongoing states of emergency, killings, massacres, torture, collusion between British state security forces and loyalist paramilitary groups, as well as the infiltration of republican groups.[11] Communities were placed under siege, monitored and surveilled for decades. According to Privacy International, British militarism in the north of Ireland was a key factor that spurred UK companies to manufacture more and more surveillance equipment.[12]

11 The Pat Finucane Centre, 2017, 'Legacy of Colonialism', https://www.patfinucanecentre.org/legacy-colonialism [Accessed March 12 2021].

12 Privacy International, July 2016, 'The Global Surveillance Industry'. Page 31.

POLICE SPYING

In the late 1960s, as revolution and rebellion erupted across the world, a specialist undercover police unit was created in Britain with a mandate to spy on groups on the left.[13] Throughout the 1970s, undercover officers from the Special Demonstration Squad (SDS) infiltrated anti-racist, black liberation, Irish solidarity, working-class, Marxist and anarchist movements.[14]

In the 1970s and 80s the British Intelligence Services set up a Subversion in Public Life Committee to spy on those involved in industrial agitating.[15]

The 1980s was a period of intense struggle by Black and Brown communities in Britain against the institutionalised racism of the British state. The SDS responded in the '80s and '90s by spying on these communities intensively. It has recently been revealed that SDS and the National Public Order Intelligence Unit (NPOIU) targeted the families of people of colour killed by the police.[16] The NPOIU also spied on the the family of Stephen Lawrence, who were trying to get justice after their son was killed in a racist attack in London in the 1990s. Their campaign attracted police surveillance after it threatened to expose institutional racism in London's Metropolitan Police.[17]

Undercover police also posed as members of ecological and animal liberation direct action movements throughout the 1990s, often using the tactic of entering into intimate relationships with female political organisers in order to gain information. The officers didn't revel their true identities to their partners.[18] These tactics continued at least until the revelation of the extent of police spying in the late 2000s.

Undercover tactics have been used alongside overt surveillance of social movements. In the 2000s the police began heavily using Forward Intelligence Teams (FIT), who would follow political organisers overtly, often appearing with long-lens cameras at protests or political meetings.[19] According to Richard Purssell, an

13 *PA News*, 2020, 'Shadowy police unit set up amid 1960s Vietnam war protests', ***Grampian Online***. https://www.grampianonline.co.uk/news/national/shadowy-police-unit-set-up-amid-1960s-vietnam-war-protests-5460/, [Accessed March 12 2021].

14 Undercover Research Group, November 2020, 'One hundred new political groups named as spycops targets' https://undercoverresearch.net/2020/11/02/more-groups-named-as-spycops-targets , [Accessed March 12 2021].

15 Undercover Research Group, June 2020, 'State Surveillance in 1984 – Union Organising as 'conspiracy', https://undercoverresearch.net/2020/01/06/state-surveillance-in-1984-trade-union-organising-as-conspiracy/ [Accessed March 12 2021].

16 Undercover Research Group, October 2019, 'How many black families were targeted by undercover officers?', https://undercoverresearch.net/2019/10/23/black-justice-campaigns/ [Accessed March 12 2021].

17 Evans, R. 2019, 'Black undercover officer who spied on Stephen Lawrence campaign named', ***The Guardian,*** https://www.theguardian.com/uk-news/2019/jul/16/black-undercover-officer-who-spied-on-stephen-lawrence-campaign-named, [Accessed March 12 2021].

18 Undercover Research Group, March 2019, "James Blond' - #spycop infiltrating animal right groups', https://undercoverresearch.net/2019/03/01/james-blond-spycop-infiltrating-animal-rights-groups/ [Accessed March 12 2021]. and Steel, H, 2014, 'I feel violated', ***The Guardian*** https://www.theguardian.com/uk-news/2014/aug/29/helen-steel-relationship-undercover-police-feel-violated [Accessed March 12 2021].

19 Anderson, T. 2013, 'Chapter 16: "When Co-Option Fails" in Fisher, R. 'Managing Democracy, Managing Dissent', ***Corporate Watch,*** https://corporatewatch.org/wp-content/uploads/2017/09/MDMD-Master-PDF1.pdf [Accessed March 12 2021].

anti-militarist organiser who was followed extensively by FIT teams at anti-militarist protests in London in 2009:

> *"They are there to intimidate you from protesting, from being part of the awkward squad. There is a clear message that they are onto you."*[20]

LEGISLATION TO TARGET DISSENT

Successive British governments have used legislation to criminalise different forms of dissent which are seen as a threat to the status quo, and to criminalise certain communities. The Conservative governments of the 1980s and '90s targeted the rights of trade unionists to strike, put in place repressive stop and search powers targeting Black and Muslim communities,[21] and introduced a new Public Order Act which included measures specifically intended to control political protests and criminalise squatters and Gypsy, Roma and Traveller communities.[22]

In 2000 the Labour government pushed through a repressive Terrorism Act, which among other deeply concerning elements, made it illegal to support various groups – including leftwing groups - that Britain considers to be terrorists. Support was described in the broadest of terms. For example, the Act makes it an offence to wear items of clothing that might indicate support for ac group featured on the list.[23] Several of Britain's non-white communities – including supporters of the Tamil and Kurdish freedom movements - have faced criminalisation ever since.[24]

20 The Guardian, October 2009, 'Police spotter card G: Richard Purssell', https://www.theguardian.com/uk/2009/oct/27/police-spotter-card-richard-purssell [Accessed March 12 2021].

21 Casciani, D. 2002. 'Troubled history of stop and search', ***BBC News***, http://news.bbc.co.uk/1/hi/uk/2246331.stm [Accessed March 12 2021].

22 Anderson, T. 2013, 'Chapter 16: "When Co-Option Fails" in Fisher, R. 'Managing Democracy, Managing Dissent'.

23 CAMPACC: Campaign Against Criminalising Communities, 'Proscribed groups', Campacc.org.uk, http://campacc.org.uk/index.php?page-proscribed-groups[Accessed March 12 2021] and Gov.uk, 2000, 'Terrorism Act 2000' ***Legislation.gov.uk*** https://www.legislation.gov.uk/ukpga/2000/11/section/13 [Accessed March 12 2021].

24 CAMPACC: Campaign Against Criminalising Communities, 'Communities targeted for harassment and prosecutions', ***Campacc.org.uk*** http://campacc.org.uk/index.php?page-anti-terror-laws-and-communities [Accessed March 12 2021].

> Political policing - Schedule 7 of the Terrorism Act

Schedule 7 came into force as part of the UK's Terrorism Act in 2000 and allows the police to stop people on arrival to, or departure from, the UK and question them in order to determine whether they might be involved preparing terrorist acts. Unlike other powers of police questioning, under Schedule 7 it is illegal to answer 'No Comment' or not to respond. People may be arrested, prosecuted and imprisoned if they refuse to give an answer. Although the questions have to be related to the investigation of terrorism, in reality people have been asked questions on a range of subjects unrelated to outlawed 'terrorist' organisations. For example, people have been questioned about their religious beliefs, personal life, participation in protests and political organising, among other personal matters. Under Schedule 7, the police also have the power to confiscate electronic devices and demand passwords, and have the power to arrest if passwords are not given.[25]

Kevin Blowe, coordinator of Network for Police Monitoring (Netpol), told Shoal Collective:

> *"By far the greatest use of Schedule 7 is against Muslims with political views, especially on foreign policy or security issues. It is a fundamentally Islamophobic policing power. However, as a tool, this power is targeting surveillance at anyone whose politics have the imagination to look beyond borders: so solidarity with migrants or independence struggles, such as the Palestinians or the Kurds. This also means gatherings of campaigners from different countries who reject capitalism's role in solutions to climate change, conflict or global poverty. This is why it is impossible to see the use of Schedule 7 as anything other than blatant political policing."*[26]

The Regulation of Investigatory Powers Act 2000 increased covert police surveillance powers, and made it a criminal offence not to disclose passwords for electronic devices to the police in certain circumstances.[27]

British police began using the term 'domestic-extremism' during the 2000s to describe supporters of left-wing movements, direct action campaigns, protest groups, and the far right. Those dubbed domestic extremists have been subjected to excessive police surveillance[28] and have been vilified in the media. According to Netpol the label has a ***"chilling"*** effect on ***"participation in public protest***

25 Gov.uk, 2000, 'Terrorism Act 2000' Legislation.gov.uk and Gov.uk, 2000, 'Schedule 7', Legislation.gov.uk, https://www.legislation.gov.uk/ukpga/2000/11/schedule/7 [Accessed March 12 2021] and Cooper, T and Anderson, T, February 2013, 'Schedule 7 of the Terrorism Act 2000: A police snooping tool to protect private profit', ***Corporate Occupation***, https://corporateoccupation.org/2013/02/27/schedule-7-of-the-terrorism-act-2000-a-police-snooping-tool-to-protect-private-profit/ [Accessed March 12 2021].

26 Quote given to Shoal Collective by Kevin Blowe, coordinator of Network for Police Monitoring, 2020.

27 Gov.uk, 2000, 'Regulation of Investigatory Powers Act 2000', Legislation.gov.uk, https://www.legislation.gov.uk/ukpga/2000/23/contents [Accessed March 12 2021].

28 Network for Police Monitoring, January 2020, 'Domestic Extremism', Netpol.org, https://netpol.org/domestic-extremism/ [Accessed March 12 2021].

and campaigns" and constrains ***"the fundamental values that lie at the heart of a fair and free society"***.[29]

The Labour government's PREVENT programme[30] brought state surveillance in Britain to a new deeply troubling level. It became mandatory for civil servants, such as teachers, medical professionals and other staff employed by the state to report any behaviour which they considered to be suspicious to the authorities, under the logic that in doing so they may pre-empt an impending terrorist attack.[31] PREVENT was strengthened by successive Conservative governments[32] and in effect, today, PREVENT places a statutory duty on civil servants to spy and report on people in settings such as schools and universities, during medical appointments, or while in hospital. According to Netpol, PREVENT ***"criminalises legitimate dissent by collecting intelligence about the thoughts and beliefs of individuals who are not involved in criminal activity"***.[33]

PREVENT's draconian powers were strengthened by the Conservative government's Counter-Terrorism and Security Act, which was passed in 2015.[34] This Act also made it compulsory - in many cases - for communication service providers to retain and hand over information about users' Internet Protocol (IP) addresses, making it easier to link individuals to particular electronic devices and locations.[35]

29 *Ibid.*

30 Full Fact, August 2017, 'What is the Prevent strategy?', Fullfact.org, https://fullfact.org/law/what-prevent-strategy/ [Accessed March 12 2021].

31 Gov.uk, 2019, 'Revised Prevent duty guidance: for England and Wales', https://www.gov.uk/government/publications/prevent-duty-guidance/revised-prevent-duty-guidance-for-england-and-wales [Accessed March 12 2021].

32 Network for Police Monitoring, June 2018, 'PREVENT', Netpol.org, https://netpol.org/campaigns/prevent/ [March 12 2021] and Economic and Social Research Council, August 2015, 'PREVENT', Esrc.ukri.org, https://esrc.ukri.org/public-engagement/social-science-for-schools/resources/prevent-the-uk-s-counter-terrorism-strategy/ [Accessed March 12 2021].

33 Network for Police Monitoring, June 2018, 'PREVENT', Netpol.org.

34 Gov.uk, 2015, 'Counter Terrorism and Security Bill', Legislation.gov.uk, https://www.gov.uk/government/collections/counter-terrorism-and-security-bill [Accessed March 12 2021].

35 Home Office, July 2016, 'Counter Terrorism and Security Bill', Gov.uk, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/540538/CTS_Bill_-_Factsheet_5_-_IP_Resolution_v2.pdf [Accessed March 12 2021].

> The Investigatory Powers Act; a mandate for a surveillance state

In December 2016, the UK parliament passed the Investigatory Powers Act,[36] which gives police forces and intelligence officers the legal right to ***"hack into computers, networks, mobile devices, servers... This could include downloading data from a mobile phone that is stolen or left unattended, or software that tracks every keyboard letter pressed being installed on a laptop".***[37] Dubbed a "snoopers' charter",[38] it shows the lengths to which the British government is prepared to go to spy on the British population, in particular organisers of social movements, journalists and lawyers acting on their behalf. Civil rights organisation, Liberty, stated that the Investigatory Powers Act allows the government ***"to spy on every one of us, violating our rights to privacy and free expression".***[39]

The government responded to the COVID-19 health crisis by passing a Coronavirus Act. The Act is supposed to only be in force temporarily,[40] but Big Brother Watch has called its restrictions the ***"most draconian powers ever in peace-time Britain"***.[41] The Act has been used extensively to ban protests and arrest demonstrators.[42] Meanwhile, police forces have ramped up surveillance during COVID-19 by massively increasing the use of surveillance drones,[43] while data from the NHS Test and Trace App – which has been downloaded by over 20 million people[44] - has also been made available to the police.[45]

36 UK Parliament, 2017, Parliament.uk https://publications.parliament.uk/pa/bills/lbill/2016-2017/0040/17040.pdf [Accessed March 12 2021].

37 Burgess, M. 2017, 'What is the IP Act and how will it affect you?', ***Wired UK***, https://www.wired.co.uk/article/ip-bill-law-details-passed [Accessed March 12 2021].

38 Griffin, A. 2016, 'Britain just got perhaps the most intrusive spying powers ever seen', ***The Independent***, https://www.independent.co.uk/life-style/gadgets-and-tech/news/snoopers-charter-2-investigatory-powers-bill-parliament-lords-what-does-it-mean-a7423866.html [Accessed March 12 2021].

39 Perraudin, F, July 2019, 'Liberty loses high court challenge to snooper's charter', ***The Guardian***, https://www.theguardian.com/law/2019/jul/29/liberty-loses-high-court-challenge-to-snoopers-charter [Accessed March 12 2021].

40 Big Brother Watch, February 2021, 'Emergency Powers and Civil Liberties report, February 2021', ***Bigbrotherwatch.org***, https://bigbrotherwatch.org.uk/wp-content/uploads/2021/03/Emergency-Powers-and-Civil-Liberties-Report-FEB-2021.pdf [Accessed March 16 2021], Page 8.

41 Big Brother Watch website homepage, 2021, ***Bigbrotherwatch.org,*** https://bigbrotherwatch.org.uk/ [accessed 16 March 2021].

42 Anderson, T, September 2020, 'The British police are using COVID-19 measures to criminalise dissent, we need to fight back', ***The Canary,*** https://www.thecanary.co/opinion/2020/09/09/the-british-police-are-using-covid-19-measures-to-criminalise-protest-we-need-to-be-ready-to-fight-back/ [Accessed 16 March 2021].

43 See Chapter 2.

44 Mageit, S, January 2021, 'UK Government Reports Test and Trace reaching record number of people', Healthcare IT News, https://www.healthcareitnews.com/news/emea/uk-government-reports-nhs-test-and-trace-reaching-record-number-people [Accessed 16 March 2021].

45 BBC News, October 2020, 'Coronavirus: Police get access to NHS Test and Trace self-isolation data', ***BBC News,*** https://www.bbc.co.uk/news/uk-54586897 [accessed 16 March 2021].

At the time of writing this report, protests were underway against the 2021 Police, Crime, Sentencing & Courts Bill. If passed, the Act will be the biggest clampdown on freedom to protest in the UK since the Public Order Act. The proposal is to amend the Public Order Act, giving police greater powers to place restrictions on public gatherings, arrest protesters for being noisy, criminalise trespass and expand stop and search powers. Heftier sentences will be given for assaulting police officers, and a new statutory offence of public nuisance will be created, punishable by up to ten years in prison.[46]

The Bill threatens to further criminalise the UK's Gypsy, Roma and Traveller communities, who could face prosecution or imprisonment for setting up camps on privately owned land.[47] The No Fixed Abode Travellers and Supporters Collective made the following statement:

> *"It is a fact that our absolute right as human beings to travel nomadically is being questioned and this is not ok! No one should be questioned, controlled, arrested or have their homes seized for choosing a nomadic lifestyle."*[48]

The Bill is also designed as an authoritarian response to the Black Lives Matter movement's tearing down of statues that commemorate Britain's racist history. It proposes making the damaging of national monuments punishable by up to tens years imprisonment.[49]

46 Norden. J. March 2020, 'Pritti Patel's new policing bill is threatening our right to protest', The Canary, Disponible en: https://www.thecanary.co/uk/analysis/2021/03/15/priti-patels-new-policing-bill-is-threatening-our-right-to-protest/ [Accessed March 12, 2021].

47 UK Parliament, 2021, 'Police, Crimes, Sentencing and Courts Bill, Parliament.uk, https://publications.parliament.uk/pa/bills/cbill/58-01/0268/200268.pdf [Accessed March 16 2021].

48 No Fixed Abode Travellers and Supporters, Undated, 'Campaigns', <https://nfats1.wixsite.com/nfatscollective/campaigns> [Accessed 17 March 2021].

49 UK Parliament, 2021, 'Police, Crimes, Sentencing and Courts Bill, Parliament.uk, <https://publications.parliament.uk/pa/bills/cbill/58-01/0268/200268.pdf> [Accessed March 16 2021].

GIVING THE GO-AHEAD TO MORE SURVEILLANCE

At the same time as the Bill was being read in parliament, a report was released by Her Majesty's Inspectorate of Constabulary (HMIC) making a number of recommendations, including proposing the continued use of high-tech surveillance technologies such as facial recognition and drones against protesters.[50] The report also sets out a strategy for a new era of police surveillance, through the National Police Coordination Centre's Strategic Intelligence and Briefing team (NPoCC SIB). The NPoCC SIB will gather information from different police forces about dissent in the UK, and ***"take national responsibility for protest-related intelligence"***.[51]

According to Kevin Blowe of Netpol, the report:

> ***"[gives] the green-light to more surveillance on campaigners and a new label – "aggravated activists". It essentially resurrects the National Public Order Intelligence Unit – the disgraced protest surveillance unit that employed undercover officers".***[52]

In March 2021 the Conservative government pushed another bill – dubbed the Spy-cops Bill - through parliament that authorises covert agents, such as police officers, MI5 agents, or military personnel, to legally carry out what would usually be considered criminal conduct. Crucially, the Covert Human Intelligence Sources Bill gives undercover police a green-light to continue deceiving women into sexual relationships.[53]

MASS SURVEILLANCE MAKING A MOCKERY OF THE HUMAN RIGHTS ACT

Repealing the Act would remove many legal protections and give free reign for the expansion of the surveillance state,[54] but new technology deployed by the state makes a mockery of these 'rights' and allows for mass surveillance on an unprecedented level. In 2020 Boris Johnson's Conservative government announced plans to repeal the UK's Human Rights Act following the UK's exit from the European Union.[55] A review of the Act is currently underway.[56] Repealing the Act would remove many legal protections and give free reign for the expansion of the surveillance state.

50 Her Majesty's Inspectorate of Constabulary (HMIC), March 2021, 'Getting the balance right? An inspection of how effectively the police deal with protests', ***Justiceinspectorates.gov.uk***, https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/getting-the-balance-right-an-inspection-of-how-effectively-the-police-deal-with-protests.pdf [Accessed 11 March 2020].

51 ***Ibid***, page 7.

52 Quote obtained by telephone from Kevin Blowe of Netpol by Shoal Collective, March 17 2020.

53 Egret, E. January 2021, 'The most dangerous law of our time continues to be pushed through parliament', ***The Canary,*** https://www.thecanary.co/uk/analysis/2021/01/13/the-most-dangerous-law-of-our-time-continues-to-be-pushed-through-parliament/ [Accessed 16 March 2021].

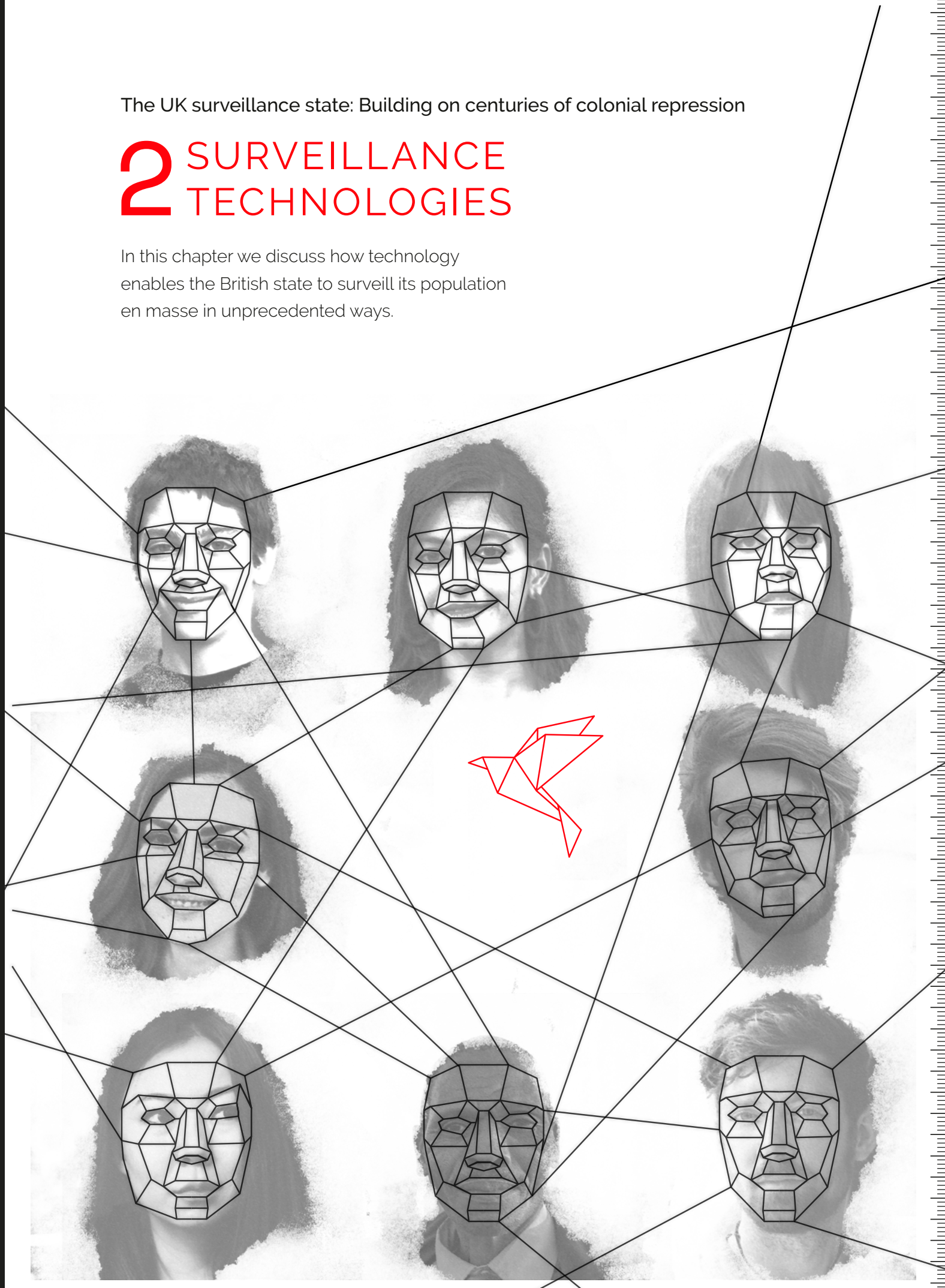
54 Liberty, Undated, 'A private and family life',***Libertyhumanrights.org.uk***, https://www.libertyhumanrights.org.uk/right/a-private-and-family-life/ [Accessed March 12 2021].

55 Boffey, D. October 2020, 'Boris Johnson set for compromise on Human Rights Act – EU sources', ***The Guardian***, https://www.theguardian.com/politics/2020/oct/07/boris-johnson-set-to-make-compromise-on-human-rights-act-eu-source [Accessed March 12, 2021].

56 Allen, K, 2021, 'The government is hell-bent on diluting the Human Rights Act. We must protect it', ***MSN***, https://www.msn.com/en-gb/news/other/the-government-is-hell-bent-on-diluting-the-human-rights-act-we-must-protect-it/ar-BB1ec8G6 [Accessed March 12 2021].

2 SURVEILLANCE TECHNOLOGIES

In this chapter we discuss how technology enables the British state to surveill its population en masse in unprecedented ways.



GOVERNMENT HACKING

In 2013, whistle-blower Edward Snowden revealed that the UK's intelligence, cyber and security agency, known as the Government Communications Headquarters (GCHQ), was tapping fibre-optic cables to collect huge amounts of internet users' personal data through its Tempora computer system. This data was also shared with the US National Security Agency (NSA).[57] Tempora intercepts phone calls and accesses phone data,[58] and the Snowden leak revealed that GCHQ took advantage of 'leaky' phone apps to access information about phone users' age, sex and location.[59] The agency can also activate a person's phone while it is turned off, and turn on a device's microphone in order to listen in on conversations.[60] GCHQ has intercepted users' data as it passes between Google servers, and has spied on 1.8 million webcam users, saving images of those having conversations.[61]

POLICE HARVESTING OF DATA FROM SEIZED DEVICES

When people are arrested, stopped at UK borders or their homes are raided, the police often seize phones, tablets, computers, memory cards and SIM cards, in order to extract personal data. A number of companies supply equipment to the UK police to do this, including Cellebrite, Digital Detective, ElcomSoft, Grayshift, Magnet Forensics, MSAB, OpenText, and Oxygen Forensics.[62]

Various police forces in the UK use technology developed by Israeli company, Cellebrite, to unlock and extract data from smartphones,[63] enabling them to crack passwords and extract contact lists, call history, internet history, calendar entries, emails, SMS messages, documents, photos and videos, as well as see what apps were used and the data stored on them. Cellebrite's technology also

57 MacAskill, E. Borger, J. Hopkins, N. Davies, N. Ball, J. June 2013, 'GCHQ taps fibre-optic cables for secret access to world's communications', ***The Guardian***, https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa [Accessed March 12 2021].

58 Gallagher, R. 2014, 'The Inside Story of How British Spies Hacked Belgium's Largest Telco', ***The Intercept***, https://theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story/ [Accessed March 12 2021].

59 Ball, J. 2014, 'Angry Birds and 'leaky' phone apps targeted by NSA and GCHQ for user data', ***The Guardian*** , https://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data [Accessed March 12 2021].

60 Amnesty International, 2015, 'Ten Spy programmes with silly codenames used by GCHQ and NSA'. ***Amnesty.org,*** https://www.amnesty.org/en/latest/campaigns/2015/03/10-spy-programmes-with-silly-codenames-used-by-gchq-and-nsa/ [Accessed March 12 2021].

61 ***Ibid.***

62 MSAB company website: https://www.msab.com/company, https://www.msab.com/products/xry/, https://www.msab.com/products/xry/xry-cloud/, Digital Detective company website: https://www.digital-detective.net/about-us/executive-team/, ElcomSoft company website: https://www.elcomsoft.co.uk/company.html, Oxygen Forensics company website: https://www.oxygen-forensic.com/en/company, GrayShift company website: https://www.wired.co.uk/article/police-iphone-hacking-grayshift-graykey-uk, Magnet Forensics company website: https://www.magnetforensics.com/for-police-leaders all undated and [accessed March 16 2021] and Scottish Parliament Reports. 2019, 'Report on Police Scotland's proposal to introduce the use of digital device triage systems (cyber kiosks)', https://digitalpublications.parliament.scot/Committees/Report/JSP/2019/4/8/Report-on-Police-Scotland-s-proposal-to-introduce-the-use-of-digital-device-triage-systems--cyber-kiosks-#Digital-device-triage-systems---cyber-kiosks [Accessed 16 March 2021].

63 Cellebrite, Undated, 'Cellebrite Mobile Forensics Tool Demonstration', Youtube.com, https://www.youtube.com/watch?v=5fEYqpJ6Mrw [Accessed March 12 2021] and Privacy International, April 2020, 'Are UK police accessing your cloud apps?', Privacyinternational.org, https://privacyinternational.org/report/3551/are-uk-police-accessing-your-cloud-apps [Accessed March 12 2021].

allows police forces to gain information regarding location, and can retrieve hidden files and deleted content.

In 2018, Privacy International reported that over half of UK police forces had confirmed that they use mobile phone extraction technology,[64] while in Scotland, media cooperative The Ferret revealed in 2017 that ***"[i]n the last three years Police Scotland have successfully obtained data from at least 35,973 phones... In the same period the police tackled 16,587 computers".***[65]

EXTRACTION OF DATA FROM THIRD PARTY SERVERS

Cloud extraction technology is designed to extract personal data stored on third party servers such as Dropbox, Slack, Instagram, Twitter and Facebook, My Activity, Uber and Hotmail. Privacy International describes cloud extraction technology as the ***"secret tech that lets government agencies collect masses of data from your apps".***[66]

Private police contractor Cellebrite claims in a video promoting its Universal Forensic Extraction Device (UFED) Cloud technology that through use of the UFED Cloud one can ***"get access to data that no longer resides on the physical device by retrieving cloud backups. In addition, UFED Cloud allows you to view a user's digital activity and locations across multiple devices, computers and tables from cloud sources such as Facebook, iCloud and Google".***[67] Cellebrite's technology also has the capability to use facial recognition when analysing photos extracted from cloud storage.[68]

Privacy International explains that this technology enables the police to continually track someone. ***"By acquiring the login credentials, it allows its users to then continue to track the online behaviour of the device's user even if you are no longer in possession of the phone".***[69] Moreover, "***the individual themselves will never know that someone has access to and may be using their cloud profile***".[70] Privacy International also points out that with access to someone's login details or cloud-based accounts, it is possible to impersonate them and send messages as if they are from the owner of the device.[71]

64 Privacy International, March 2018, 'Digital stop and search: how the UK police can secretly download everything from your mobile phone', ***Privacyinternational.org***, https://privacyinternational.org/report/1699/digital-stop-and-search-how-uk-police-can-secretly-download-everything-your-mobile [Accessed March 12 2021].

65 Tibbitt, A, 2017, 'Everything Police Scotland can find out about you from your mobile phone'. ***The Ferret***, https://theferret.scot/privacy-mobile-phones-cellebrite-police-scotland/ [Accessed March 12 2021] and ***Freedom of Information*** (FOI) request made by The Ferret in March 2017 https://www.documentcloud.org/documents/3938332-17-0297-Final-Response.html [Accessed March 12 2021].

66 Privacy International, January 2020, 'Cloud extraction technology: the secret tech that lets government agencies collect masses of data from your apps', Privacyinternational.org, https://privacyinternational.org/long-read/3300/cloud-extraction-technology-secret-tech-lets-government-agencies-collect-masses-data [Accessed March 12 2021].

67 Cellebrite, Undated, Cellebrite.com, www.cellebrite.com/en/ufed-cloud-analyzer-5/ [Accessed October 2020] and Cellebrite's YouTube channel: https://www.youtube.com/watch?v=dJbl8Tiz3-k [Accessed March 12 2021].

68 Privacy International, January 2020, 'Cloud extraction technology: the secret tech that lets government agencies collect masses of data from your apps'.

69 *Ibid.*

70 *Ibid.*

71 *Ibid.*

SPYING ON SECURE MESSAGING

Several companies advertise the potential to spy on secure messaging services such as Signal and Telegram. Russian company ElcomSoft, for example, states that its technology can ***"enable experts to gain access to password-protected, locked and encrypted information contained in a range of mobile devices and cloud services".***[72] ElcomSoft's Phone Viewer 5.0 technology can, in theory, view Telegram and Signal private messenger conversations.[73] It lists several police forces, as well as the Serious Fraud Office and the Ministry of Defence, among its clients.[74]

MONITORING COMMUNICATIONS

An IMSI-catcher is a mass surveillance tool, which is used by the police to monitor phones. It masquerades as a mobile phone tower and phones may connect to it automatically or unknowingly, but in so doing, the IMSI - International Mobile Subscriber Identity – number, which is unique to each SIM card, is recorded and may be used by the police to trace the phone owner's identity.[75]

According to Privacy International: "IMSI-catchers are indiscriminate surveillance tools that could be used to track who attends a political demonstration or a public event like a football match. They can even be used to monitor your calls and edit your messages – and you wouldn't even know it was happening".[76] Moreover, The Intercept found that IMSI-catchers can potentially install malware onto a person's phone.[77]

Towards the end of 2015, VICE News and Privacy International detected an IMSI-catcher being used on an anti-austerity protest in London. When questioned about it, a police officer at the scene said that he would 'neither confirm nor deny' its use.[78] Subsequently, Vice and Privacy International sent FOI requests to police forces across the UK, all of which declined to confirm whether they were using IMSI-catchers. The Bristol Cable, however, found that in 2015, London's Metropolitan Police paid more than £1m to CellXion, which manufactures IMSI-catchers. The payment was for Covert Communications Data Capture (CCDC) technology.

72 ElcomSoft, Undated, https://www.elcomsoft.co.uk/company.html, Elcomsoft.co.uk, [Accessed March 12 2021].

73 ElcomSoft, Undated, 'Phone Viewer 5.0 gains the ability to display conversation histories and secret chats in Telegram - Help Net Security. Help Net Security', https://www.helpnetsecurity.com/2020/04/30/elcomsoft-phone-viewer-5-0/ [Accessed March 12 2021].

74 ElcomSoft, Undated, https://www.elcomsoft.co.uk/company.html, Elcomsoft.co.uk.

75 Privacy International, August 2018, 'IMSI Catchers', Privacyinternational.org, https://www.privacyinternational.org/explainer/2222/imsi-catchers [Accessed March 12 2021].

76 Privacy International, August 2018, 'IMSI Catchers', Privacyinternational.org.

77 Zetter, K. 2020, 'What Are Stingrays and Dirtboxes?', ***The Intercept***, https://theintercept.com/2020/07/31/protests-surveillance-stingrays-dirtboxes-phone-tracking/ [Accessed March 12, 2021].

78 Vice News, 2016, 'Phone Hackers: Britain's Secret Surveillance', Vice.com, https://www.vice.com/en/article/9kjxe7/phone-hackers-britains-secret-surveillance [Accessed March 12 2021].

Avon & Somerset Police and West Midlands Police also bought CCDC technology from CellXion.[79] Further investigations by the Bristol Cable have found that at least nine UK police forces have purchased IMSI-catchers. Another FOI request by The Ferret in 2016 revealed that the Scottish Prison Service (SPS) had been using IMSI-catchers to block prisoners' outgoing calls.[80]

FACIAL SEARCHING AND THE POLICE NATIONAL DATABASE

All UK police forces, as well as several other government agencies, can search the Police National Database (PND) using a 'facial searching' tool, which relies on Facial Recognition Technology (FRT).[81] he PND contains over 3.5 billion local police records[82] and roughly 100,000 new images are uploaded every month.[83] Use of the PND is governed by the Data Protection Act and the Human Rights Act, and the police are meant to use it only for the purposes of investigating or preventing criminal or civil offences. In practice, however, these powers can be very broadly interpreted.[84] Facial searching' allows police and other state agencies to search photographs on the PND of people who have been arrested in the UK, including people who have never been convicted of any crime.[85] This technology allows the police to match CCTV images with images stored on the PND using FRT.[86] Making FRT available through the aforementioned Database has cost the UK Home Office – namely, taxpayers - £1.1 million.[87] According to the Home Office, the private companies running the PND only have access to the database software but not to its contents.

79 Aviram A. 2016, 'Revealed: Bristol's police and mass mobile phone surveillance', ***The Bristol Cable,*** https://thebristolcable.org/2016/10/imsi/ [Accessed March 12 2021].

80 Rigg. J. May 2017, 'Stringray phone tracker use in the UK admitted for the first time', ***Engadget.com,*** https://www.engadget.com/2016-05-27-stringray-phone-tracker-uk.html?guce_referrer=aHR0cHM6Ly9kdWNrZHVja2dvLmNvbS8_cT1IYXJyaXMrc3RpbmdyYXkrVXNlK2luK1VLJnQ9bG0maWEgd2Vi&guce_referrer_sig=AQAAALgfOke7VVDu8-oBzRCYZFG1Wnui3B7QGtUlDr3NMYikFZr6B4iv0lkEv55HozGK497J3pG4KFkCnLyERHf-Fo7drn2rRWQWAOagVQUn53cTLZiFxOLORJpaaSkcJmf1SOJzKx6SERjMkfkidaddblbzJ7l3pP6ofkxGLhRtETfl&guccounter=2 [Accessed March 12 2021] and Aviram, A, 2016, ***'IMSI catchers: a campaign for police to come clean on mass mobile phone surveillance', The Bristol Cable,*** https://thebristolcable.org/imsi/ [Accessed 16 March 2021].

81 Home Office, 2019, 'Team H. Fact Sheet on live facial recognition used by police', Homeofficemedia.blog.gov.uk, https://homeofficemedia.blog.gov.uk/2019/09/04/fact-sheet-on-live-facial-recognition-used-by-police/ [Accessed March 12 2021].

82 Babuta. A, September 2020, 'Big Data and Policing', ***Rusi.org***, https://rusi.org/sites/default/files/201709_rusi_big_data_and_policing_babuta_web.pdf [Accessed March 12 2021].

83 FOI request made by Pippa King to the Home Office in 2015, https://www.whatdotheyknow.com/request/263544/response/665587/attach/2/20150616%20Response%20Letter%2035046.pdf [Accessed 16 March 2021].

84 Gov.uk, 2010, 'On the Operation and Use of the Police National Database. National Policing and Improvement Agency', Gov.uk, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/243554/9999102808.pdf [Accessed March 16. 2021.

85 BBC News, September 2017, 'Facial recognition database 'risks targeting innocent people'. ***BBC News***, https://www.bbc.co.uk/news/amp/uk-41262064 [Accessed March 12 2021].

86 Babuta. A, September 2020, 'Big Data and Policing', Rusi.org.

87 FOI request made by Pippa King to the Home Office in June 2015, https://www.whatdotheyknow.com/request/263544/response/665587/attach/2/20150616%20Response%20Letter%2035046.pdf [Accessed March 16 2021].

RETROSPECTIVE FACIAL RECOGNITION

Six UK Police forces use 'retrospective facial recognition'.[88] According to HMIC this method:

> *"uses images caught by a camera, later comparing them against a large database of facial images held by the police to try to identify them".*[89]

'Retrospective facial recognition' allows the police to compare images to databases other than the PND.

THE USE OF LIVE FACIAL RECOGNITION BY UK POLICE FORCES

Live Facial Recognition (LFR) is the real-time application of FRT. According to Science Focus magazine: ***"Live facial recognition (LFR), also known as automatic facial recognition, identifies people in a video in real time, using a set of photographs as a reference. When used in public, cameras scan a crowd and the software highlights any matches between members of the public and the people in their database".***[90]

LFR is currently used by just five UK police forces, while 25 forces plan to trial the technology.[91] South Wales Police and London's Metropolitan Police have trialled the technology most extensively:

South Wales Police has used LFR on 61 occasions since 2017 at concerts, in shopping centres, at sporting events and at least one political protest.[92] In 2018, it arrested 22 people after they were identified through LFR.[93] The LFR software is provided by the Japanese electronics giant NEC.[94]

The Metropolitan Police says that it uses NEC's NeoFace LFR technology,[95] and has used LFR on at least 17 occasions between 2016 and 2020, including in the busy shopping streets of Oxford Circus,[96] in Romford town centre, and around Stratford's Westfield shopping centre.[97]

88 ***HMIC,*** 'Getting the balance right', 2021, Page 47.

89 ***Ibid***.

90 Rigby, S., 2019. ***Live facial recognition: how is it used? BBC Science Focus Magazine,*** https://www.sciencefocus.com/future-technology/live-facial-recognition-how-is-it-used/ [Accessed 16 March 2021]

91 ***HMIC,*** 'Getting the balance right', 2021, Page 47.

92 South Wales Police, Undated, 'Court of Appeal Judgment', Afr.south-wales.police.uk, https://afr.south-wales.police.uk/blog/court-of-appeal-judgment/ [Accessed March 12 2021].

93 South Wales Police, Undated, 'What is AFR?', Afr.south-wales.police.uk, https://afr.south-wales.police.uk/ [Accessed March 12 2021].

94 South Wales Police, Undated, 'Home', Afr.south-wales.police.uk, https://www.south-wales.police.uk/en/news-room/introduction-of-facial-recognition-into-south-wales-police/ [Accessed March 12 2021].

95 Metropolitan Police, 2021, 'Update on facial recognition', Met.police.uk, https://www.met.police.uk/advice/advice-and-information/facial-recognition/live-facial-recognition-trial/ [Accessed 16 March 2021].

96 FOI Request made to the Metropolitan Police in February 2020, https://www.whatdotheyknow.com/request/648561/response/1610448/attach/5/20%2003%2006%20LFR1%20URN%202020%20002%20BOOTH%20FOIA%20REDACTED%20WAD%20Q1.PDF.pdf?cookie_passthrough=1

97 Vincent, J. 2020, 'London police to deploy facial recognition cameras across the city', ***The Verge*** https://www.theverge.com/2020/1/24/21079919/facial-recognition-london-cctv-camera-deployment [Accessed 16 March 2021].

LFR has also been used by police in Hull, Leicestershire and Liverpool, and in public places such as Hull Docks and the Download Music Festival, where 90,000 people were checked against the Europol EU-wide database.[98]

LFR has also been used by police in Hull, Leicestershire and Liverpool, and in public places such as Hull Docks and the Download Music Festival, where 90,000 people were checked against the Europol EU-wide database.[99]

AUTOMATIC NUMBER PLATE RECOGNITION (ANPR)

Police in the UK have been using Automatic Number Plate Recognition (ANPR) technology since the 1990s,[100] and the system has been rolled out nationwide since 2006.[101] Forces reportedly have access to images from a network of 14,000 cameras[102] producing 50 million ANPR 'read records' daily. The Home Office recently awarded a contract to multinational arms giant BAE Systems to provide a new National ANPR System, at a cost of £14 million. The system went live in 2019.[103]

98 Big Brother Watch, Undated, 'Stop Facial Recognition', Bigbrotherwatch.org.uk, https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/ [Accessed 16 March 2021].

99 Big Brother Watch, Undated, 'Stop Facial Recognition', Bigbrotherwatch.org.uk.

100 Big Brother Watch, Undated, 'Police use of ANPR', Bigbrotherwatch.org, https://bigbrotherwatch.org.uk/wp-content/uploads/2013/03/ANPR-Report.pdf [Accessed 16 March 2021].

101 The Independent, 2005. '*Surveillance UK: why this revolution is only the start', Independent Online Edition, Science & Tech,* https://web.archive.org/web/20080103025848/ http://news.independent.co.uk/sci_tech/article334684.ece [Accessed 16 March 2021].

102 Trendall, S. 2018. 'Home Office rolls on with £14m project to replace police number-plate database', https://publictechnology.net/articles/news/home-office-rolls-%C2%A314m-project-replace-police-number-plate-database [Accessed 16 March 2021].

103 BAE Systems, 2020, 'Transforming nationwide automatic number plate recognition, https://www.baesystems.com/en/cybersecurity/feature/transforming-nationwide-automatic-number-plate-recognition-anpr, [Accessed 16 March 2021].

DRONES

UK police have used small remote-controlled drones since November 2015, when they were jointly used by Devon & Cornwall Police and Dorset Police.[104] They are increasingly used for surveillance in search and rescue operations and in monitoring crime scenes but are also used regularly to monitor political protest,[105] and are being regularly deployed to monitor COVID-19 lockdowns.[106] Half of the UK's police forces reportedly use drones,[107] many on a daily basis,[108] and many use drones that are equipped with thermal imaging technology.

According to figures obtained under FOI from Avon & Somerset constabulary, there was a 47.3 percent increase in the use of drones by the force over the period March–June 2020, during the UK's first Coronavirus lockdown, compared to March–June 2019. The force used drones 103 times in the first six months of 2020, meaning that sometimes drone flights occurred on an almost daily basis.[109] This increase was likely due to lockdown enforcement measures. South Wales Police also reported a substantial increase in the use of drones during the first COVID-19 lockdown, compared to previous months.[110] Derbyshire Police controversially used a drone to shame people out walking their dogs in the Peak District during lockdown,[111] while Surrey Police played a recorded message from a drone, ordering groups to disperse over the 2020 Easter weekend.[112] West Midlands police and Greater Manchester police used drones equipped with thermal imaging cameras to monitor illegal raves during August 2020.[113]

104 Langford, E. 2020. 'Home Office Plans To Use Military-Grade Drones To Pursue Suspects And Monitor Protests Are Raising Privacy Concerns', ***Politics*** Home, https://www.politicshome.com/news/article/military-grade-drones-home-office [Accessed 16 March 2021].

105 HMIC, 'Getting the balance right', 2021, Page 42.

106 FOI request made by Tom Anderson to Kent Police in July 2020. https://www.whatdotheyknow.com/request/676655/response/1616941/attach/html/4/20%2007%200870%20Appendix.xlsx.html [Accessed 16 March 2021].

107 Heliguy, 2018. 'Drones a game-changer, say police', Heliguy.com, https://www.heliguy.com/blog/2018/12/12/drones-a-game-changer-say-police/ [Accessed 16 March 2021].

108 FOI request by Tom Anderson to Avon & Somerset Police in August. 2020 https://www.whatdotheyknow.com/request/use_of_drones_2019_20_25#incoming-1626855 [Accessed 16 March 2021].

109 FOI request by Tom Anderson to Avon & Somerset Police in August 2020, https://www.whatdotheyknow.com/request/use_of_drones_2019_20_25#incoming-1626855 and Anderson, T. 2020, 'Avon and Somerset Constabulary's use of drones almost doubled over lockdown', ***The Canary*** https://www.thecanary.co/investigation/2020/11/25/avon-and-somerset-constabularys-use-of-drones-almost-doubled-over-lockdown/ [Accessed 16 March 2021].

110 FOI request by Tom Anderson to South Wales Police, October 2020, https://www.whatdotheyknow.com/request/676650/response/1671179/attach/4/Response%20639%2020.pdf

111 Leprince-Ringuet, D. 2020, 'Police drones are taking to the skies', ***ZDNet,*** https://www.zdnet.com/article/police-drones-are-taking-to-the-skies/ [Accessed 16 March 2021].

112 Langford, E. 2020. 'Home Office Plans To Use Military-Grade Drones To Pursue Suspects And Monitor Protests Are Raising Privacy Concerns', ***Politics Home.***

113 BBC News, 2020, 'Manchester city-centre rave condemned by police', ***BBC News*** https://www.bbc.com/news/uk-england-manchester-55459614 [Accessed 16 March 2021].

Many of the drones used in the UK are supplied by Chinese company DJI.[114] with the Mavic 2 Enterprise being one of the typical drone models currently used by British police. It reportedly ***"costs around £2,800, weighs less than a kilogram, and has a 29-minute battery life with an operating range of 5km"***, according to an article by Eleanor Langford in Politics Home.[115]

The UK National Police Air Service (NPAS) is considering buying much larger Hermes 900 drones from Israeli company Elbit Systems,[116] despite the fact that the Hermes drone has been developed and tested in a context of an ongoing war against the Palestinian people.[117] The Israeli Hermes 900 drone ***"has a 15-metre wingspan, weighs 970kg, and can fly for up to 36 hours at altitudes of 30,000 feet."***[118] One of the justifications given by NPAS for considering these drones is their potential in monitoring demonstrations.[119]

^ **The Parrot Anafi** drone, in use by South Wales Police. Source: Wikimedia Commons/Dottensm Creative Commons License: BY-SA 4.0

> **Hermes** drones from Elbit Systems. Source: Wikipedia Commons

114 See Cleveland Police Drone Unit's Twitter. February 2020 https://twitter.com/DronesPolice/status/1227877097768726528, (Matrice is a DJI model), also FOI request made by Tom Anderson to South Wales Police in October 2020, https://www.whatdotheyknow.com/request/676650/response/1671179/attach/4/Response%20639%2020.pdf, and Kent Police website, Undated, 'Unmanned Aerial Vehicles', https://www.kent.police.uk/foi-ai/kent-police/who-we-are/who-we-are-and-what-we-do/unmanned-aerial-vehicle-drones/, [All accessed 16 March 2021].

115 Langford, E. 2020. 'Home Office Plans To Use Military-Grade Drones To Pursue Suspects And Monitor Protests Are Raising Privacy Concerns', ***Politics Home.***

116 Lewis, S, 2020, 'National Police Air Service tests potential of drone technology', Commercial Drone Professional, https://www.commercialdroneprofessional.com/national-police-air-service-tests-potential-of-drone-technology/ [Accessed 16 March 2021] and Asa Winstanley, 2020, 'British police may deploy Israeli drone used to kill Palestinians'***, The Electronic Intifada,*** https://electronicintifada.net/blogs/asa-winstanley/british-police-may-deploy-israeli-drone-used-kill-palestinians [Accessed 16 March 2021].

117 Stop the Wall, 2015, Supporting Israeli apartheid: EU funding for Elbit Systems, ***Stopthewall.org,*** Page 9 https://www.stopthewall.org/sites/default/files/horizon2020%20elbit.pdf [Accessed 16 March 2021], and Drone Wars UK, 2010, 'Israel and the Drone Wars', Page 7. https://dronewarsuk.files.wordpress.com/2014/01/israel-and-the-drone-wars.pdf [Accessed 16 March 2021].

118 Langford, E. 2020. 'Home Office Plans To Use Military-Grade Drones To Pursue Suspects And Monitor Protests Are Raising Privacy Concerns', ***Politics Home.***

119 *Ibid.*

3 THE STATE AND CORPORATIONS – TWO SIDES OF THE SAME COIN

The massive increase in the use of high-tech surveillance by police forces and state agencies is being advocated for and advanced by two main actors. The first is the state itself, which is hungry for more and more effective ways to monitor and control the population. The second is private companies, which stand to make massive profits from marketing the new technology. These two actors are mutually supportive of each other. The different branches of the state in the UK ensure that companies will profit from new tenders for surveillance technology, while in turn the UK government is lobbied by private companies to relax legal restrictions on the use of new technology. At the same time, the details of the police's use of surveillance technology are often kept a secret from the public, citing national security considerations.

This chapter examines the close relationship between corporations and the UK government, and the current lack of restrictions on the use of facial recognition technology, among other aspects of high-tech surveillance.

THE 'REVOLVING DOOR'

It is unsurprising that the interests of the state and private companies coincide with regard to surveillance technology. There is a 'revolving door' between the offices of companies producing high-tech' surveillance technology and Westminster. For example, Campaign Against Arms Trade has shown that between 2007 and 2020, at least 31 people either moved from jobs at BAE Systems to government or civil service positions, or vice-versa. On top of that, the company was given over a thousand hours of government time in the form of meetings between the company and government departments.[120] This close relationship has clearly paid off for BAE. For example, it recently received a multi-million pound contract for the nationwide Automatic Number Plate Recognition system.[121]

The British government is keen to promote the success of UK surveillance companies abroad, too. For example, British company FaceWatch has exported facial recognition technology from the UK to Brazil, and has benefited from support from the Department of International Trade.[122]

120 Campaign Against the Arms Trade, Undated, 'Influence', Caat.org.uk, https://caat.org.uk/data/influence/org/3/meetings, [Accessed 16 March 2021].

121 See Chapter 2.

122 FOI request made by Jo Griffin to the Department of International Trade in 2019, https://www.whatdotheyknow.com/request/626720/response/1499993/attach/html/3/Final%20response%2005672.pdf.html [Accessed 16 March 2021].

In the wake of the COVID-19 pandemic, the UK government made deals with private companies which involved making available massive amounts of National Health Service (NHS) patients' data to these companies. This data is supposed to remain under the control of the NHS, but the deals have been criticised for not taking into account privacy concerns. A public petition by Open Democracy argued: ***"The COVID-19 datastore will hold private, personal information about every single one of us who relies on the NHS. We don't want our personal data falling into the wrong hands".***[123] One of the companies which received a contract was Faculty, a company specialising in artificial intelligence. Faculty is linked to Dominic Cummings, who was Prime Minister Boris Johnson's Chief Adviser at the time. Faculty received £1.1m for its services to the NHS.[124]

LOBBYING FOR UNRESTRICTED SURVEILLANCE

Private companies use their unrestricted access to government decision-makers to lobby against restrictions on the use of surveillance technology. For example, companies that are involved in the manufacturing of drones are lobbying the UK's Civil Aviation Authority to lift restrictions on the flying of large unpiloted aircraft.[125] BAE Systems and US partner General Atomics are pushing for their 'Protector' drone to be able to fly in civilian airspace.[126] In turn, the Ministry of Defence (MOD) mirrors these requests by also pushing for changes in regulations surrounding airspace to enable the testing of the drone. Ultimately, the MOD wants the Protector to be deployed ***"across the full spectrum of operations"***, including for: domestic security purposes such as surveillance; training of personnel; and being available to civil authorities for contingencies and emergencies.[127]

123 Open Democracy, 2020, 'Stop the secrecy: Publish the NHS COVID data deals', https://www.opendemocracy.net/en/stop-secrecy-publish-nhs-covid-data-deals/ [Accessed 16 March 2021].

124 Open Democracy, 2020. 'Under pressure, UK government releases NHS COVID data deals with big tech', https://www.opendemocracy.net/en/ournhs/under-pressure-uk-government-releases-nhs-covid-data-deals-big-tech/?s=09&fbclid=IwAR23ZvPYNzrjlbktmXasn4jLt8O96999e4-tMDhofUqX9Vsf_68R94DiedA, [Accessed 16 March 2021].

125 Drone Wars UK, 2019, 'General Atomics bring in BAE Systems to lobby for 'Protector' drone to fly in UK' https://dronewars.net/2019/01/28/general-atomics-bring-in-bae-systems-to-lobby-for-protector-drone-to-fly-in-uk/#more-11122 [Accessed 16 March 2021].

126 Drone Wars UK, 2019, 'General Atomics bring in BAE Systems to lobby for 'Protector' drone to fly in UK.'

127 Drone Wars UK, 2019, 'Take Action: Military drone use within UK', https://dronewars.net/military-drones-in-uk/ [Accessed 16 March 2021].

FACIAL RECOGNITION - AN UNREGULATED TECHNOLOGY

Currently, there are no legal limitations on the use of facial recognition technology (FRT) in the UK,[128] although the UK's Information Commissioner says that the images captured should be subject to the same Data Protection regulations as all types of images, and should be considered "sensitive data".[129]

In 2019, a cross-party group of Westminster MPs signed a letter calling for an immediate halt to the use of FRT until regulations are put in place.[130] An Automated Facial Recognition Technology (Moratorium and Review) Bill passed the first reading in the House of Lords in 2019, but has made no further progress.[131]

The Scottish parliament has called for the police in Scotland not to use FRT, until they have demonstrated a legal basis for its use.[132] In 2020, the Scottish Parliament's Justice Sub-Committee on Policing published a report saying that there was no legal basis for Police Scotland's plans to begin using the technology. Police Scotland has agreed not to purchase LFR technology, at least for the time being.[133]

Companies are taking advantage of the gap with regard to regulation of FRT and are seizing the opportunity to market their products to authorities in the UK. For example, FaceWatch markets its facial recognition technology to the UK police and local authorities. In 2018, officers from Essex Police tweeted about attending a trial of FRT organised by FaceWatch, which was also attended by staff from Southend Council.[134]

128 Big Brother Watch, Undated, 'Stop Facial Recognition', https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/ [Accessed 16 March 2021].

129 Information Commissioner's Office, 2019, 'The use of live facial recognition technology by law enforcement in public places' https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion20191031.pdf [Accessed 16 March 2021].

130 Dearden, L. 2019, 'Police may have used 'dangerous' facial recognition unlawfully in UK, watchdog says', ***The Independent,*** https://www.independent.co.uk/news/uk/home-news/facial-recognition-uk-police-london-law-information-commissioner-latest-a9180101.html [Accessed 16 March 2021].

131 UK Parliament, 2019, 'Automated Facial Recognition Technology (Moratorium and Review) Bill [HL] - Parliamentary Bills', ***Services. parliament.uk,*** https://services.parliament.uk/bills/2019-19/automatedfacialrecognitiontechnologymoratoriumandreview.html [Accessed 16 March 2021].

132 Thomas, E. 2020. 'Facial recognition is in London. So how should we regulate it?' ***Wired UK,*** https://www.wired.co.uk/article/regulate-facial-recognition-laws [Accessed 16 March 2021].

133 Lynch, E. 2020. 'The Use of Live Facial Recognition Technology in Scotland: A New North-South Divide?' - ***UK Human Rights Blog,*** https://ukhumanrightsblog.com/2020/02/25/the-use-of-live-facial-recognition-technology-in-scotland-a-new-north-south-divide/ [Accessed 16 March 2021].

134 FOI request made by Pippa King to Southend on Sea Borough Council in July 2018, https://www.whatdotheyknow.com/request/facial_recognition_demonstration?unfold=1#incoming-1186570 [Accessed 16 March 2021].

In 2019 Waltham Forest Council in London carried out a three day Live Facial Recognition (LFR) trial. The technology for the trial was provided free of charge by Israeli company AnyVision. By providing the trial for free, AnyVision was clearly trying to get a foot in the door in order to access the lucrative UK local government procurement market.[135]

UK POLICE PUSHING AHEAD WITH LFR DESPITE COURT RULING

Ed Bridges is a member of the public whose face was captured with LFR by South Wales Police while attending a protest in Cardiff, and again when he was out shopping. He brought a case against South Wales Police, claiming that the use of the technology had breached his right to privacy.[136] The court initially found in favour of the police but in August 2020, Mr. Bridges won his case in an appeal brought before the High Court. Liberty, which represented Bridges, stated at the time that The High Court's ruling means that South Wales Police's use of LFR should be halted.[137]

Bridges said after the hearing: *"This technology is an intrusive and discriminatory mass surveillance tool. For three years now South Wales Police has been using it against hundreds of thousands of us, without our consent and often without our knowledge. We should all be able to use our public spaces without being subjected to oppressive surveillance".*[138]

Liberty lawyer Megan Goulding said: *"The Court has agreed that this dystopian surveillance tool violates our rights and threatens our liberties… It is time for the Government to recognise the serious dangers of this intrusive technology. Facial recognition is a threat to our freedom – it needs to be banned".*[139]

135 Barnes, S. 2019, 'London council used facial recognition technology on streets without consulting residents.' *The Telegraph,* https://www.telegraph.co.uk/news/2019/10/07/london-council-used-facial-recognition-technology-streets-without/ [Accessed 16 March 2021].

136 The Times, 2019, 'Ed Bridges's challenge against facial recognition technology heads to Court of Appeal', https://www.thetimes.co.uk/article/ed-bridgess-challenge-against-facial-recognition-technology-heads-to-court-of-appeal-skjgdbhgd [Accessed 16 March 2021].

137 *Ibid.*

138 *Ibid.*

139 *Ibid.*

In response to the High Court's judgement, however, the Metropolitan Police issued a statement saying that its LFR policy is ***"different"*** to that of the South Wales Police, making clear that it would carry on using it.[140] South Wales Police also said that it will review its policy in light of the judgement, but will continue to develop the use of the technology.[141]

In 2021, the report by Her Majesty's Inspectorate of Constabulary (HMIC) further responded to Bridges' case. The report discusses the High Court's judgement, and concludes:

> *"On balance, we believe that this technology has a role to play in many facets of policing, including tackling those protesters who persistently behave unlawfully. We expect to see more forces begin to use facial recognition as the technology develops."*[142]

Despite the High Court Ruling, and public and parliamentary and concerns over LFR, HMIC made "supporting forces to use live facial recognition technology" one of its key recommendations in its March 2021 report on policing protest.[143]

140 Metropolitan Police UK, Undated, 'Update on facial recognition', Met.police.uk, https://www.met.police.uk/advice/advice-and-information/facial-recognition/live-facial-recognition/ [Accessed 16 March 2021].

141 South Wales Police, Undated, 'What is AFR?', Afr.south-wales.police.uk.

142 HMIC, 'Getting the balance right', ***2021,*** page 45.

143 Ibid, page 5.

THE UK POLICE'S CULTURE OF SECRECY OVER SURVEILLANCE TECHNOLOGY

While researching this report Shoal Collective made Freedom of Information (FOI) requests to police forces across the UK. We were met with a culture of secrecy regarding the use of surveillance technology. The strict control of information available to the public about surveillance contrasts sharply with the unfettered access to the government, which is enjoyed by the companies marketing the technology.

> Drones:

Although police did release some information about the overt use of drone technology, none of the police forces that we contacted disclosed information about their covert use, citing national security issues.[144]

London's Metropolitan Police refused to release the information that we requested under FOI, claiming that: ***"to disclose the dates [that the force] used overt drones during 2019–2020, either operationally or in testing, would identify specific operations, which could undermine our law enforcement functions".***[145]

We also asked the Metropolitan Police under FOI whether drone technology, or drones using thermal imaging, had been used in the surveillance of Black Lives Matter (BLM) protests in London in 2020. The Met said that it had not used these technologies overtly, but cited the threat of terrorism as a reason to refuse to disclose whether drones had been used covertly for this purpose. The response reads: ***"Whilst not questioning the motives of the applicant, confirming or denying that any other information is held regarding the use of any specialist equipment for covert purposes, would show criminals what the capacity, tactical abilities and capabilities of the force are, allowing them to target specific areas of the UK to conduct their criminal/terrorist activities. Confirming or denying the specific circumstances in which the police service may or may not deploy such technologies, would lead to an increase of harm to covert investigations and compromise law enforcement".***[146]

Avon & Somerset Constabulary refused to tell us which company manufactured its drones, claiming that: ***"disclosing information that would allow the identification of force UAVs could compromise their operational purpose and allow them***

144 For example see the FOI request made by Tom Anderson to Kent Police in August 2020, https://www.whatdotheyknow.com/request/676655/response/1616941/attach/html/3/20%2007%200870%20Response%20Letter.pdf.html and FOI request made by Tom Anderson to Kent Police, in September 2020, https://www.whatdotheyknow.com/request/676655/response/1633213/attach/html/4/20%2007%20870%20IR%20Response%20Letter.pdf.html [All accessed 16 March 2021].

145 FOI request made by Tom Anderson to the Metropolitan Police in September 2020, https://www.whatdotheyknow.com/request/use_of_drones_by_the_met#incoming-1631947 [Accessed 16 March 2021].

146 FOI request made by Tom Anderson to the Metropolitan Police in October 2020, https://www.whatdotheyknow.com/request/surveillance_at_blm_protests#incoming-1667206 [Accessed 16 March 2021].

to be targeted".[147] Similarly, South Wales Police refused to give us information about how often they used drones covertly, or which ones they used. Finally, we asked Thames Valley Police under FOI whether drone technology had been used against environmental protectors who have been living in tree houses to protest the HS2 high speed railway. Again, we received a response that police could *"neither confirm nor deny"* whether drones had been used.[148]

> Facial Recognition Technology:

We submitted FOI requests to the police, seeking information on the use of FRT and were also met with similar responses. We requested that the Metropolitan Police tell us under FOI whether FRT had been used in the surveillance of BLM protests in London in 2020. The Met responded that it had not used these technologies overtly, but refused to say whether they had been used covertly, citing the threat of *"terrorist activities".*[149] Similarly Avon and Somerset Constabulary refused to answer whether the force used automatic facial recognition in its covert operations, or whether FRT had been used covertly in the policing of BLM protests in Bristol in 2020.[150] Thames Valley Police and Kent Police also refused to answer our questions about FRT.[151]

147 FOI request made by Tom Anderson to Avon & Somerset Police in August 2020, https://www.whatdotheyknow.com/request/use_of_drones_2019_20_25#incoming-1626855 , [Accessed 16 March 2021].

148 FOI request made by Eliza Egret to Thames Valley Police in November 2020, https://www.whatdotheyknow.com/request/696654/response/1669501/attach/3/3924%2020%20TVP%20Final%20Response%20Letter.pdf?cookie_passthrough=1, [Accessed 16 March 2021].

149 FOI made by Tom Anderson to the Metropolitan Police in September 2020, https://www.whatdotheyknow.com/request/use_of_drones_by_the_met#incoming-1631947 [Accessed 16 March 2021].

150 FOI request made by Tom Anderson to Avon & Somerset Constabulary in July 2020, https://www.whatdotheyknow.com/request/use_of_facial_recognition_techno_2#followup and August 2020, https://www.whatdotheyknow.com/request/blm_protests_2021#incoming-1644735 [Both accessed 16 March 2021].

151 FOI request made by Eliza Egret to Thames Valley Police in November 2020, https://www.whatdotheyknow.com/request/696654/response/1669501/attach/3/3924%2020%20TVP%20Final%20Response%20Letter.pdf?cookie_passthrough=1 [Accessed 16 March 2021]

> IMSI Catchers:

When campaigners seek to challenge the police's refusal to disclose information about the UK surveillance state, the available appeal mechanisms are often insufficient. For example, Privacy International has worked tirelessly to attempt to force the UK police to be more transparent about their use of IMSI-catchers, bringing several appeals to the Information Rights Tribunal. Sadly the tribunal upheld the police's ***'neither confirm or deny'*** policy.[152]

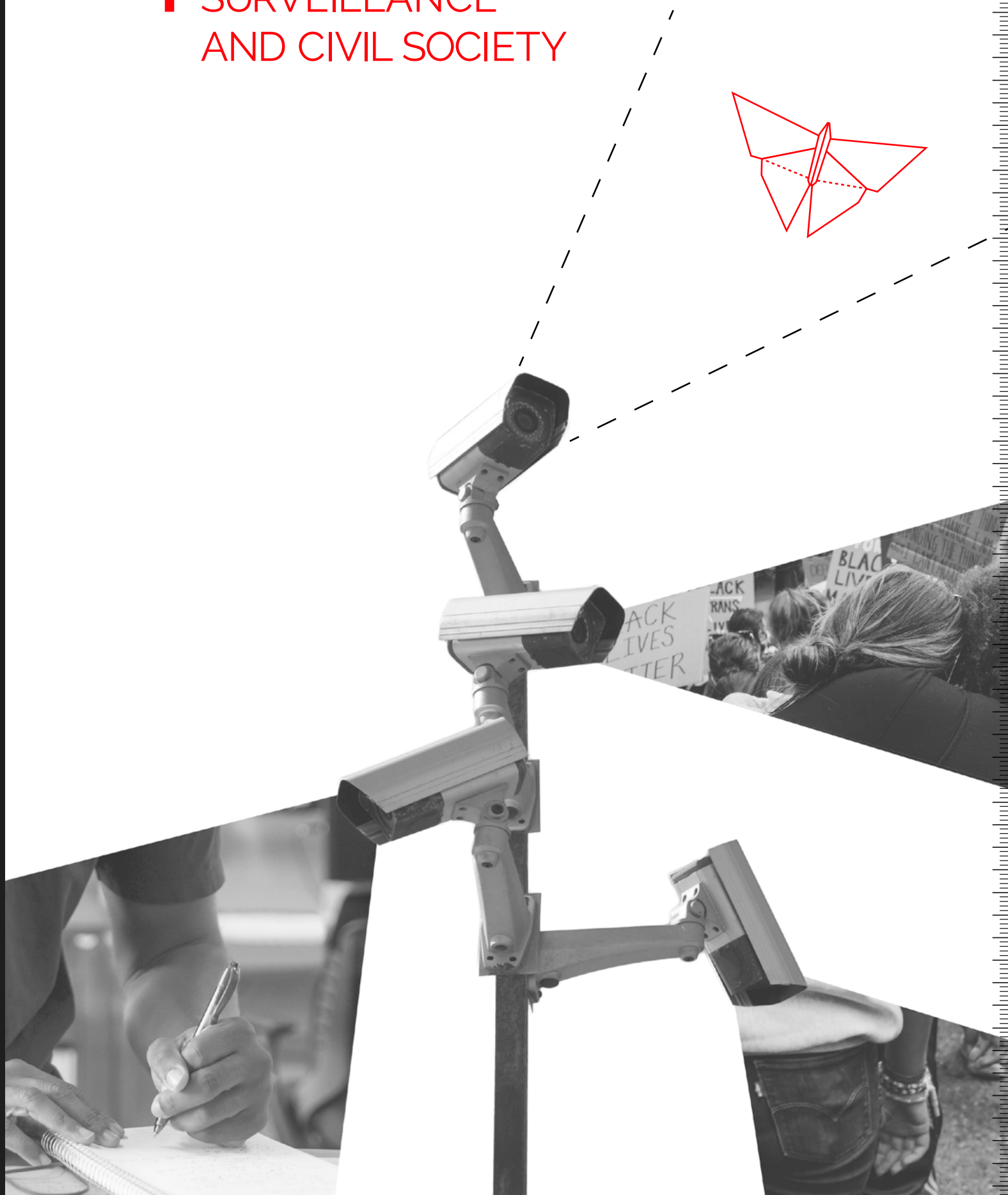
Therefore, it's no surprise that in November 2020 the Metropolitan Police told us that it would ***"neither confirm nor deny"*** whether IMSI-catchers had been used on Black Lives Matter protests throughout that year.[153]

Black Lives Matter protesters in London's Oxford Street Font: Alisdare Hickson Flickr

152 Privacy International, 2019, 'Information Tribunal Decisions re IMSI Catchers: A loss for transparency and why we will continue the fight through other means', https://privacyinternational.org/long-read/3925/information-tribunal-decisions-re-imsi-catchers-loss-transparency-and-why-we-will [Accessed 16 March] 2021].

153 FOI request made by Eliza Egret to the Metropolitan Police in November 2020, https://www.whatdotheyknow.com/request/imsi_catcher_use_on_blm_protests?nocache-incoming-1682649#incoming-1682649

4 THE CHILLING EFFECT – SURVEILLANCE AND CIVIL SOCIETY



The exponential growth of high-tech surveillance in the UK has had a chilling effect on grassroots movements fighting for social change. As we discussed earlier, UK social movements have historically been subjected to repression, police surveillance and criminalisation. Many such movements have been targeted by state-orchestrated campaigns to delegitimise their supporters by labelling them terrorists or domestic extremists, despite any evidence to support those claims.[154]

The proliferation of new technologies available to the state has opened up fresh avenues for repression on a massive scale where whole communities, populations or movements can be surveilled without ever realising that they have been targeted. As will be shown below, its negative effects are often felt most strongly by working class communities and people of colour.

In this chapter we will give some examples of the effect of these new technologies on dissent in the UK, paying particular attention to the classed and racialised dimension of the use of this technology.

POLICE POWERS BEING USED TO CARRY OUT 'DIGITAL STRIP SEARCHES'

In the UK, police are empowered to seize electronic devices when people are under arrest, during house raids and when people are stopped under Schedule 7 of the Terrorism act at UK borders.[155] Alastair Lyon of Birnberg Peirce solicitors believes that Schedule 7 is often used to carry out a "digital strip search" of activists. Lyon told Shoal Collective:

> *"The definition of terrorism is wide enough that huge areas of legitimate political activity can fall within it. Schedule 7 interview answers can't generally be used in court. The process of asking questions does not appear to be the purpose of most stops: answers given in interviews themselves are probably of least interest to the police. The 'digital strip search' appears to be the point. Confiscated digital devices can be detained for a maximum of seven days, unless retained thereafter for a criminal investigation. Devices give the police access to huge parts of your life and relationships. This is key: the police are potentially creating a huge database of this information".*[156]

Once police have seized devices, they are able to use data extraction services provided by companies like Cellebrite[157] to monitor people's personal data. These 'digital strip searches' have become an important tool in the repression of organisers involved in social movements.

154 See Chapter 1.

155 Network for Police Monitoring, 2012, 'Schedule 7 terror laws used to interrogate activists', https://netpol.org/2012/12/12/schedule-7-terror-laws-used-to-interrogate-activists/ [Accessed 16. March 2020].

156 Interview carried out by Shoal Collective with Alastair Lyon of Birnberg Peirce solicitors, 2020.

157 See Chapter 2.

POLICE MONITORING OF COMMUNICATIONS HAVING A "CHILLING EFFECT ON PROTESTS"

New technologies like IMSI-catchers have a significant impact on the right to privacy, by covertly acquiring personal data through mobile phones, making it almost impossible to be anonymous in a crowd.[158] The data acquired may be used to monitor a person's activities and build up a profile. Shoal Collective spoke to Llia Siatitsa, Programme Director of Privacy International, who explained how technologies such as IMSI-catchers affect people's ability to organise:

> *"New surveillance technologies are radically transforming the ability of authorities to monitor protests. They are already capable of conducting generalised, invisible, real-time surveillance of protests, from a distance, without people knowing or consenting by using new technologies, such as IMSI-catchers. Planning and participating in protests requires us to communicate freely and confidentially without unlawful interference. So far, most of these surveillance technologies have been deployed with no transparency or an appropriate legal framework and oversight. The use of such intrusive technologies is a serious and unjustified interference with our privacy, but also can directly infringe our freedom to assemble and have a chilling effect on protests as it dissuades people from participating".*[159]

158 See Chapter 2.

159 This quote was obtained by Shoal Collective part of the research for this report, and the account and views expressed are solely those of the interviewee.

LIVE FACIAL RECOGNITION AND THE THREAT TO DISSENT

Daragh Murray, co-author of a 2019 Essex University report on Live Facial Recognition, explains the repressive potential of its use:

> *"Live facial recognition (LFR) interferes with the right to a private life – but the impact of this technology extends far beyond this right. LFR technology identifies a person in real time using biometric processing. Combining LFR with other data sources can reveal much about a person's professional and private life... Detailed individual profiles made possible by advanced facial recognition may be used to inform diverse decisions relating, for example, to the rights to work, to health, or to social welfare. What will it mean for how people engage with those around them, if all of their activities are recorded, and used to inform potentially life changing decisions about them? A real concern is that people will be afraid of engaging at the fringes of society, and that they will modulate their behaviour towards the mainstream."*[160]

It is clear that one of the functions of LFR for London's Metropolitan Police and South Wales Police is the control of political dissent. For example, police in Wales used LFR in a security operation for a royal visit in 2018. Such visits have previously been the subject of political controversy and protest.[161] In March 2018, South Wales Police deployed a police van equipped with LFR cameras to monitor an anti-militarist protest outside the Defence Procurement, Research, Technology & Exportability (DPRTE) arms exhibition at Cardiff's Motorpoint Arena.[162]

Facial Recognition Technology being used to monitor protesters by South Wales Police. Source: Emily Apple of the Network for Police Monitoring (with permission)

160 University of Essex, 2019, 'Live facial recognition: the impact on human rights and participatory democracy', https://www.essex.ac.uk/blog/posts/2019/11/07/live-facial-recognition-the-impact-on-human-rights-and-participatory-democracy [Accessed 16 March 2021].

161 South Wales Police, April 2020, 'All Deployments', *Afr.south-wales.police.uk,* https://afr.south-wales.police.uk/wp-content/uploads/2020/04/All-Deployments.pdf [Accessed 16 March 2021].

162 Apple, E. 2018, 'South Wales Police under fire for using facial recognition technology against protesters', *The Canary,* https://www.thecanary.co/uk/2018/03/29/south-wales-police-under-fire-for-using-facial-recognition-technology-against-protesters/ [Accessed 16 March 2021].

— In 2020, the Metropolitan police chose to run a Facial Recognition trial in Oxford Circus in an area that is often used for political protests.[163]

— In 2017, the Metropolitan Police used LFR to monitor the annual Remembrance Day ceremony. The force admitted that people who were not wanted for arrest were on an LFR 'watchlist', because the police suspected they might disrupt the 'security plan' for the event.[164] This shows that police are not going to be content with using LFR technology to identify wanted people, but will cast their nets much more broadly in terms of surveillance and data collection. They could potentially use LFR to make pre-emptive arrests, and to harass those they deem to be disruptive.

These examples of LFR being used to target political protest are deeply concerning, and could deter people from taking part in demonstrations. The use of the technology means that it is increasingly difficult to remain anonymous while attending protests, and could mean that key organisers are singled out by the technology and subjected to police harassment.

163 FOI request made by Phil Booth to the Metropolitan Police in July 2020, https://www.whatdotheyknow.com/request/648561/response/1610448/attach/html/5/20%2003%2006%20LFR1%20URN%202020%20002%20BOOTH%20FOIA%20REDACTED%20WAD%20Q1.PDF.pdf.html [Accessed 16 March 2021].

164 FOI request by Big Brother Watch to the Metropolitan Police in March 2018, https://bigbrotherwatch.org.uk/wp-content/uploads/2018/04/Metropolitan-Police-20180300000548.pdf [Accessed 16 March 2021].

LFR: AN INACCURATE AND RACIALLY BIASED TECHNOLOGY

LFR is also extremely inaccurate with regard to identifying certain faces, showing a racial and gender bias that is very concerning and which perpetuates the existing racial and gendered discrimination that is already so deeply engrained in society. The Essex University report found that: ***"Across the six trials that were evaluated, the LFR technology made 42 matches – in only eight of those matches can the report authors say with absolute confidence the technology got it right".***[165] Big Brother Watch claims that: ***"Met Police Facial Recognition was 93% inaccurate from 2016–19"*** and that ***"3,000+ people [had been] wrongly identified by police facial recognition".***[166] A 2018 study by Massachusetts Institute of Technology (MIT) showed that the technology came up with more errors for women and for non-white people, since the dataset used to test the accuracy of the software was ***"77 per cent male and more than 83 per cent white".***[167]

Despite the mounting evidence that FRT is extremely inaccurate in identifying people's faces, other than those of white men, police in the UK have so far failed to take action to remove FRT from their digital surveillance tool kit. They continue to use technology that has a negative racial and gender bias against people of colour in particular, and women more generally.

The BBC reported in 2019 that a ***"former head of facial recognition"*** for the UK police had flagged up in 2014 ***"that ethnicity can have an impact on [facial recognition] search accuracy"***. He had asked CGI, the Canadian company managing the police's facial image database, to investigate the issue. However, the police do not appear to have followed up these concerns.[168]

HMIC's 2021 report into protest policing acknowledges that FRT technology is racially biased, but simply says that the police are continuing to work to ensure: ***"that disproportionate bias against black, Asian and minority ethnic communities is minimised".***[169] The report does not have any answers to the question of how the police are able to ensure that.

The killing of Rashan Charles, who died after being restrained by Metropolitan Police officers in 2017,[170] and the deaths of so many other people of colour at the hands of the British police[171] show how deeply racist the UK police is as an

165 Human Rights, Big Data & Technology Project, the University of Essex Human Rights Centre, 2019, 'HRBDT Researchers Launch New Report on London Metropolitan Police's Trial of Live Facial Recognition Technology' ***HRBDT,*** https://www.hrbdt.ac.uk/hrbdt-researchers-launch-new-report-on-london-metropolitan-polices-trial-of-live-facial-recognition-technology/ [Accessed 16 March 2021].

166 Big Brother Watch, Undated, 'Stop Facial Recognition', Bigbrotherwatch.org.uk.

167 Massachusetts Institute of Technology, 2018, 'Study finds gender and skin-type bias in commercial artificial-intelligence systems', https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212 [Accessed 16 March 2021].

168 White, G. 2019, 'Use of facial recognition tech 'dangerously irresponsible'', https://www.bbc.co.uk/news/technology-48222017 [Accessed 16 March 2021].

169 ***HMIC,*** 'Getting the balance right', page 48.

170 Townsend, M. 2017, 'Police watchdog calls for Met officer in custody death inquiry to be suspended', ***The Guardian,*** https://www.theguardian.com/uk-news/2017/sep/16/police-met-ipcc-custody-death-rashan-charles [Accessed 16 March 2021].

171 Inquest, 2021, 'BAME deaths in police custody', https://www.inquest.org.uk/bame-deaths-in-police-custody [Accessed 16 March 2021].

institution. People of colour are twice as likely to be shot by police in the UK than white people,[172] and a person who is Black or from an Asian background is twice as likely to die in police custody than a white person if restraint or use of force are used, or where the person under arrest is registered as having mental health difficulties.[173] It is, therefore, very unsettling that a police force that is already racially biased would rely on digital tools that are in and of themselves racially biased, in order to identify persons of interest. Such unreliable tools can only exacerbate the feelings of mistrust in the police.

The Metropolitan Police has also been using LFR in a racialised and classist manner. According to the 2011 census, in Stratford, the area of London where the Met deployed LFR three times,[174] 54% of residents were not born in the UK[175] and over 20% are Muslim. 52% of children in the Borough of Newham, the part of London where Stratford is located, live in poverty, compared to a London-wide total of 38%.[176] In 2016 and 2017, the Metropolitan Police deployed LFR technology at Notting Hill Carnival,[177] an annual festival led by members of the West Indian community. The carnival has historically been repressed by the police, and is often a flashpoint where anger against London's racialised policing spills onto the streets.[178]

Police forces in the UK already practise systemic racial violence. Add an inaccurate, racially biased algorithm to this mix, and the combination is nightmarish.

172 Qasim, W. 2020, 'The UK is Not Innocent – Police Racism Has a Long and Violent History Here Too', ***Novara Media,*** https://novaramedia.com/2020/06/01/the-uk-is-not-innocent-police-brutality-has-a-long-and-violent-history-here/ [Accessed 16 March 2021].

173 Inquest, 2021, 'BAME deaths in police custody'.

174 Big Brother Watch, Undated, 'Stop Facial Recognition'.

175 'Stratford and New Town Demographics (Newham, England)', Stratford-and-new-town.localstats.co.uk,lable at: http://stratford-and-new-town.localstats.co.uk/census-demographics/england/london/newham/stratford-and-new-town [Accessed 16 March 2021]. and Statistics, 2018, 'Population of England and Wales'. ***Ethnicity-facts-figures.service.gov.uk***, https://www.ethnicity-facts-figures.service.gov.uk/uk-population-by-ethnicity/national-and-regional-populations/population-of-england-and-wales/latest [Accessed 16 March 2021].

176 Trust for London, Undated, 'Poverty and Inequality Data For Newham', https://www.trustforlondon.org.uk/data/boroughs/newham-poverty-and-inequality-indicators/ [Accessed 16 March 2021].

177 Brown, J. 2019, 'Police use of live facial recognition technology: Challenges and concerns', ***House of Commons Library,*** https://commonslibrary.parliament.uk/police-use-of-live-facial-recognition-technology-challenges-and-concerns/ [Accessed 16 March 2021].

178 White, J. 2020, 'Police, Press & Race in the Notting Hill Carnival 'Disturbances'' ***History Workshop,*** https://www.historyworkshop.org.uk/notting-hill-carnival-disturbances/ [Accessed 16 March 2021]. and Youle. E. 2020, 'Exclusive: New Data Reveals Crime Should Not Be The Story Of Notting Hill Carnival', HuffPost UK, : https://www.huffingtonpost.co.uk/entry/notting-hill-carnival-arrest-rates-same-as-glastonbury_uk_5d5d1d18e4b063487e9519d5?guccounter=2&guce_referrer=aHR0cHM6Lyg kdWNrZHVja2dvLmNvbS8&guce_referrer_sig=AQAAAH8ymTxlUXmo5xtMZyDvhNcIJUZtsqAKiEPtf7Gw7ZuSsuKwOJtPhOnWryFyIZbe2TVc-voUA8GAvaAv_sxfROLEO85wge-aaizxKjYTsU6JzndnK2uN_vG77hSAvV2BJrTumfDgpA02UkeRJcadhj8M7hZG9_0sP_1yrjWNKcS- [Accessed 16 March 2021].

HACKING THE PHONES OF UK JOURNALISTS AND ORGANISERS

Israeli company NSO Group is one of the world's biggest manufacturers of malware. It sells the technology exclusively to governments.[179] Its Pegasus spyware is described as ***"a program so sophisticated that it can embed into your mobile phone through just one phone call, even if you don't take that call"***.[180] In 2018, Citizen Lab researchers ***"identified a total of 45 countries where Pegasus operators may be conducting surveillance operations"***, including the UK.[181] Although the nature of such technology makes it difficult to determine whether the UK government uses it to spy on British citizens, in 2020, NSO was listed as an exhibitor at the Home Office's annual Security and Policing exhibition[182] and is scheduled to appear at the 2021 International Security Expo in London.[183]

UK residents have also been subjected to incidents of cross-border hacking and surveillance, which are likely coming from foreign governments. NSO made headlines in the UK in 2018 when it was revealed that its Pegasus spyware had been used in an attempt to hack into the phone of an employee of the UK-based NGO Amnesty International.[184] In this case, a hacker used WhatsApp to try to install the malware. Had the employee clicked on a link in the WhatsApp message, their phone would have installed Pegasus without their knowledge, and had access to all the phone data.[185]

Several other UK residents have been targeted by Pegasus malware including London-based Saudi satirist Ghanem Almasarir, political activist Yahya Assiri, and Faustin Rukundo, a member of a Rwandan opposition group who is living in exile.[186]

Although the above cross-border cyber attacks were not carried out by the UK government, they show the dangerous potential of technologies like Pegasus.

179 Amnesty International, 2018, 'Meet NSO Group: a go-to company for human rights abusers', ***Amnesty.org.uk***, https://www.amnesty.org.uk/meet-nso-group-go-company-human-rights-abusers [Accessed 16 March 2021].

180 Big Brother Watch, 2019,'Surveilling journalists from inside their phones', ***Bigbrotherwatch.org.uk***, https://bigbrotherwatch.org.uk/2019/12/surveilling-journalists-from-inside-their-phones/ [Accessed 16 March 2021].

181 Marczak, B. Scott-Railton, J. McKune, S. Razzak, B. and Deibert, R. 2018, 'HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries'. ***The Citizen Lab*** https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/ [Accessed 16 March 2021].

182 Security and Policing, Undated, 'Exhibitors list 2020: NSO Group', Securityandpolicing. https://www.securityandpolicing.co.uk/exhibitors/exhibitors-list-2020/nso-group/ [accessed October 2020].

183 International Security Expo 2021, Undated, 'Exhibitors', ***Internationalsecurityexpo.com***, https://www.internationalsecurityexpo.com/exhibitors/nso-group?&azletter=N&searchgroup=libraryentry-exhibitors [Accessed 16 March 2021].

184 Amnesty International, 2018, 'Meet NSO Group: a go-to company for human rights abusers'.

185 Ibid. and Marczak, B. Scott-Railton, J. McKune, S. Razzak, B. and Deibert, R., 2018. ***HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries.***

186 Brewster, T. 2018, 'Exclusive: Saudi Dissidents Hit With Stealth iPhone Spyware Before Khashoggi's Murder', ***Forbes,*** https://www.forbes.com/sites/thomasbrewster/2018/11/21/exclusive-saudi-dissidents-hit-with-stealth-iphone-spyware-before-khashoggis-murder/?sh=7018d2f22e8b a [Accessed 16 March 2021].and Hughes, S. Evans. R. Kirchgaessner, S. 2020. 'UK to host spyware firm accused of aiding human rights abuses', ***The Guardian,*** https://www.theguardian.com/world/2020/feb/06/uk-to-host-spyware-firm-accused-of-aiding-human-rights-abuses [Accessed 16 March 2021].

ANPR SYSTEM USED TO MONITOR SOCIAL MOVEMENT ORGANISERS

En 2005, la policía detuvo al activista antimilitarista John Catt y a su hija Linda después de que su coche fuera señalado por la tecnología de Reconocimiento Automático de Matrículas (RAM). Había sido incluido en una "lista caliente" del RAM después de que la policía observara la matrícula del coche de Catt en una manifestación ante la fábrica de armas EDO MBM.

According to The Guardian:

> *"...the van had passed beneath an automatic number plate recognition (ANPR) camera in east London, triggering an alert: "Of interest to Public Order Unit, Sussex police". Within seconds Catt, 50, and her 84-year-old father, John, were apprehended by police and searched under the Terrorism Act".*[187]

Neither John nor Linda had a criminal record and they were not arrested or accused of any crime.[188]

Several other people involved in direct action movements have complained that police have stopped them repeatedly after their car had been flagged by the police. According to The Guardian - reporting in 2009 - officers were told they could ***"place "markers" against the vehicles of anyone who attends demonstrations using the national ANPR data centre in Hendon, north London, which stores information on car journeys for up to five years".***[189]

More recently, the threat of the ANPR system has been used to control people's movement during the COVID-19 lockdown. In 2020, the Welsh government threatened to use the ANPR to track cars crossing the border from England.[190] Although these travel restrictions may seem relatively benign in the context of the health crisis, the use of the ANPR as a threat shows how much power the state has to control people's movement.

187 Lewis, P. Evans, R. 2009, 'Activists repeatedly stopped and searched as police officers 'mark' cars', ***The Guardian,*** https://www.theguardian.com/uk/2009/oct/25/surveillance-police-number-plate-recognition [Accessed 16 March 2021].

188 *Ibid.*

189 *Ibid.*

190 Sheridan. E. 2020. 'Welsh police could use ANPR to identify people travelling across border from England', ***The Telegraph,*** https://www.telegraph.co.uk/politics/2020/10/15/welsh-police-could-use-anpr-identify-people-travelling-across/ [Accessed 16 March 2021].

DRONES USED TO HARASS PROTESTERS

We interviewed a participant in the 2019 Power Beyond Borders protest camp in Hertfordshire, who preferred to remain anonymous, about the effect of the use of drone technology in a protest context:

> *I took part in Reclaim the Power's mass action camp in late July 2019. It was up at Hodderston Hertfordshire, just north of London, and situated very close to Rye House power station, owned by Drax... It was at the campsite in Hodderston that I witnessed drones surveilling in the latter stage of the event.*
>
> *...at the time I saw the drones, it was daytime. I spoke with others in the camp about the drones, and they were all of a similar opinion. We all felt that their use was excessively intrusive. Likely aimed in part to make us feel uncomfortable and watched".*[191]

We were also told by those we interviewed that – in addition to the Power Beyond Borders camp – drones were used to monitor a 2020 protest held in Bristol to commemorate the death of a city resident, Anna Campbell. Anna was killed in northeast Syria (Rojava) while taking part in the armed resistance against the Turkish invasion. Animal liberationists also told us that the police had used drones to monitor attempts to sabotage the badger cull in Devon.[192] According to the 2021 HMIC report, drones were used to monitor Extinction Rebellion protesters at Bristol Airport in August 2020.[193]

191 Shoal Collective. interview with participant in the 2019 ***Power Beyond Borders*** camp conducted in August 2020.

192 Shoal Collective, interviews with campaigners, 2020.

193 ***HMIC,*** 'Getting the balance right', page 46.

CASE STUDY

The effects of police surveillance on an international supporter of the Kurdish Freedom Movement

Shoal Collective spoke to Nik Matheou, an internationalist in the Kurdish Freedom Movement based in London. He described how the movement is constantly experiencing police repression, and how the police extracted phone data in an attempt to prosecute his comrade, Josh Schoolar:[194]

> *"From late 2016, and through all of 2017, Josh was in Syria, in Rojava… He went initially to do civil volunteer work… Six months after that he decided to join the International Freedom Battalion, which is a battalion of the People's Protection Units (YPG), made up of anarchist and communist groups from Turkey and around the world. He fought with them for several months, participating in the liberation of Raqqa [from Daesh/ISIS]. After the liberation of Raqqa, he stayed for a couple of months more and then came home."*

The YPG is not an illegal terrorist group in the UK. In fact, a British jury in the case of Aidan James – another YPG fighter – found that it was not a crime for James to join the YPG's fight against Daesh.[195]

Josh had been back from Syria six months when he was stopped by the police under Schedule 7. Mattheou continued:

> *"In November 2018, we went to continental Europe. When coming back, however, we were Schedule 7 interviewed at the border in Dover. That was the beginning of the repression for Josh. He was questioned separately in a different room to us about his time in Syria… His phone was taken … and then returned to him two or three days later."*

Mattheou went on to describe how in July 2019 Josh was rearrested:

> *"He had just returned home from a Plan C festival [Plan C is an anti-authoritarian left-wing organisation]. He was arrested at home. His house was raided and his phone and laptop were taken, and he was taken in for questioning…*
>
> *His workplace was also raided by, as I understand it, armed police. Josh was a Special Needs Education teacher at a school in Manchester.*

194 This case study is based on an interview conducted as part of the research for this report, and the account and views expressed are solely those of the interviewee.

195 Judiciary UK, 2019, 'Sentencing Remarks', Judiciary.uk, https://www.judiciary.uk/wp-content/uploads/2019/11/SENTENCING-REMARKS.pdf [Accessed 16 March 2021].

His phone was taken by Manchester police, which meant that they had another opportunity to try and recover things. They claimed subsequently, through communication with his lawyer, that he had images on his phone which demonstrated that he had received weapons training in Syria. So, the phone being taken was the key evidence that they were claiming to put together. It's important to say, though, that although he remained under investigation under Section 5 of the Terrorism Act – preparing acts of terrorism – he was never charged with anything [as the YPG is not an illegal group].

The raid to his workplace alerted the school. They had actually already been told about his time in Syria. He had obtained proof of his good behaviour while he was there. There were no records that the Asayish, the police force in northern Syria, had ever had any issues with him, and he had confirmation that he had been teaching English in Kobanê. Unfortunately, the school fired him, even though he hadn't been charged by the [UK] police."

Mattheou described the effects of this repression on Schoolar's life:

"In terms of the effects on Josh's life, they were profound. I really can't believe that the raid on his school was anything other than an attempt to do what it achieved: which was to get him fired and to ruin his chance of pursuing his chosen career as a teacher. He had to radically change his outlook on what he was going to be doing in his life from that point on. It also affected his life because at that point his passport was taken away.

And it created a general problem with being able to feel confident with communication with close friends. If he was communicating with friends and then that was found out through his electronics, then potentially that could make a stronger case against them. So, he didn't do it. It was a constant low-level panic.

He lost his way of paying rent. He had to move home for several months before being able to move back to Manchester. It really defined the entire last two years of his life before he sadly passed away."

CONCLUSIONS

The British Empire used surveillance, spying, data collection and monitoring techniques for centuries to impose its rule on colonised populations and stifle dissent. However, technological advances coupled with the state's self-serving national security narratives over the last two decades have enabled the creation of a surveillance society on steroids.

State surveillance is used alongside police violence and the violence of the prison system to control dissent. The ever-encroaching surveillance state has a chilling effect on participation in social movements for change, because it enables the targeting, harassment and criminalisation of social movement organisers.

The growth of the surveillance society in the UK is being pushed forward by private companies, eager to make a profit out of the ever-increasing demand for new technologies; and by the British government, keen to control the population. These actors have overlapping interests. Private companies lobby government for less regulation on surveillance technology, while state institutions use that lack of regulation to cast the surveillance net wider.

The full extent of the police's use of surveillance technology is kept a secret from the public. This veil of secrecy is maintained by the police's 'neither confirm nor deny' responses to many public requests.

Surveillance technology is also being used in an unjust and discriminatory way against working-class people and communities of colour. Notably, UK police forces are refusing to halt their use of LFR technology, despite acknowledging that it is racially biased.

The discriminatory application of the UK's draconian terror legislation means that certain communities are treated with suspicion and criminalised. For example, Muslims, Tamil people and Kurdish people encounter even greater police surveillance by virtue of their religion or ethnicity.[196] The UK government is also pushing for new repressive trespass laws, which will destroy the livelihoods of Gypsy, Roma and Traveller communities.[197] This unequal treatment of certain communities within the UK surveillance state is a continuation of Britain's colonial legacy.

The intrusive and repressive technologies described in this report place growing power in the hands of the police and other authorities. This power has so far gone largely unchecked. The experience of mass surveillance in the UK illustrates that the monitoring of our day to day lives and the harvesting of our personal data will continue to be used to control dissent, and silence radical voices.

196 See Chapter 1.

197 No Fixed Abode Travellers and Supporters, Undated, 'Campaigns'.

It is necessary for us to fight back against the surveillance society and to resist the introduction of new technologies that will be used to control us and our communities. We need to take steps to defend ourselves against state surveillance and to stand up for those movements and communities who will bear the biggest brunt of it. This is only possible if we are able to look beyond the state's 'national security' smokescreens which are intended to isolate and divide us, and to stand in solidarity with radical social movements, working class communities and people of colour – all of whom disproportionately face state repression and criminalisation.

RECOMMENDATIONS

It is necessary to defend ourselves and our communities from state surveillance. The websites listed below offer some examples of how to do so:

- Privacytools.io provides services, tools and knowledge to protect your privacy against global mass surveillance.
- La Electronic Frontier Foundation (eff.org) provides tools to protect digital privacy and free speech.
- If you attend a political protest, then you are likely be subjected to police filming and surveillance. It is not illegal to wear a mask on a protest in the UK.[198] Take a look at this article about why people choose to wear a mask at demonstrations as a response to increased police surveillance - https://netpol.org/campaigns/protest-anonymity/

And here are a number of useful links to campaigns against different aspects of the surveillance state:

- Network for Police Monitoring (https://netpol.org/), Big Brother Watch (https://bigbrotherwatch.org.uk/) y Privacy International (https://www.privacyinternational.org/) are all great resources for monitoring and campaigning against the police state.
- Big Brother Watch's campaign on Facial Recognition Technology (https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/).
- Undercover Research Group's work on police spying (https://undercoverresearch.net).
- Netpol's campaign on UK protest surveillance (https://netpol.org/campaigns/protest-surveillance/) and useful 'know your rights' information for dealing with the police (https://netpol.org/know-your-rights/).
- Corporate Watch (corporatewatch.org) have useful information about campaigning against corporate power. They have also published a Do-It-Yourself guide to investigating companies.

198 Las máscaras son legales a menos que un oficial de policía de alto rango ordene su retirada en virtud del artículo 60 de la Ley de Orden Público de 1994. Véase Free Beagles. '***Removal of Masks, etc***', https://network23.org/freebeagles/police-powers/removal-of-masks-etc/, [Accessed 16 March 2021].

The police are the agents of the state. using technologies described in this report to monitor us. You can:

- Consider starting a 'Copwatch' group to defend your community from state surveillance and police violence.
  See https://wecopwatch.org/want-to-start-a-copwatch/
- Read Black Lives Matter's call for the defunding of the police (https://blacklivesmatter.com/what-defunding-the-police-really-means/).

Images:

Cover page:
Socialist Appeal_Black_Lives_Matter_6 June 2020, London, Flickr

Inside cover:
Lucía Armiño

Page 3:
Photomontage. Original image Pxfuel.com

Page 15:
Photomontage. Original images Pxfuel.com

Page 25:
Pxfuel.com

Page 34:
Photomontage. Font: Wikipedia Commons

Current page:
The crowd surrounding the fallen statue of slave trader Edward Colston during the Black Lives Matter protest in Bristol. Keir Gravil. Flickr

ABOUT THE ORGANIZATIONS

ENCO (European Network of Corporate Observatories) is a network of European civic and media organisations dedicated to investigating corporations and corporate power.

https://corpwatchers.eu

The **Multinationals Observatory**, based in Paris, is an online plateform that provides resources and in-depth investigations on the social, ecological and political impact of French transnational corporations.

https://multinationales.org

The Observatory of Business and Human Rights in the Mediterranean (ODHE), based in Barcelona, is a Suds and Novact project that aims to expose corporate-related human rights' impact and complicities in occupation and armed conflict contexts.

www.odhe.cat

Shoal is a radical, independent co-operative of writers and researchers. We produce news articles, investigations, analysis and theory-based writing as a contribution to, and a resource for, movements that are attempting to bring about social and political change.

www.shoalcollective.org

In association with:

NOVACT suds Internacionalisme Solidaritat Feminismes

With the support of:

Ajuntament de Barcelona ICIP Institut Català Internacional per la Pau OPEN SOCIETY FOUNDATIONS