

# CAUGHT IN THE WEB:

**'Prevent'  
databases and the  
policing of children**

# Table of Contents

|                                                                                                       |    |
|-------------------------------------------------------------------------------------------------------|----|
| List of acronyms                                                                                      | 1  |
| Executive Summary                                                                                     | 2  |
| Key findings                                                                                          | 6  |
| Introduction: What is Prevent and whom does it affect?                                                | 11 |
| How do the police store data about children and other people under Prevent? And who has access to it? | 16 |
| The starting point: Prevent Case Management Tracker                                                   | 24 |
| Data                                                                                                  | 25 |
| Collection and use of data on racial identity                                                         | 28 |
| Data input                                                                                            | 35 |
| Prevent as intelligence: The role of FIMUs                                                            | 38 |
| Progressing a referral to a Channel panel                                                             | 41 |
| Secret pathways: Transition to 'Police-Led Partnerships'                                              | 44 |
| Prevent as policing: Extending the 'spider's web'                                                     | 48 |
| Police National Computer                                                                              | 49 |
| Criminal Intelligence (CRIMINT)                                                                       | 52 |
| Police National Database                                                                              | 53 |
| Ports Authority Watchlist and the Warnings Index                                                      | 55 |
| Analysis and Conclusions                                                                              | 58 |
| The collection of race data and the monitoring of equality impacts                                    | 58 |
| Mission creep: turning Prevent into a surveillance programme                                          | 62 |
| Avoiding consent                                                                                      | 64 |
| Final comments                                                                                        | 65 |
| Recommendations                                                                                       | 66 |
| Acknowledgements                                                                                      | 68 |

# List of acronyms

|             |                                                                                                     |
|-------------|-----------------------------------------------------------------------------------------------------|
| ANPR        | AUTOMATIC NUMBER PLATE RECOGNITION                                                                  |
| BFI         | BORDER FORCE INTELLIGENCE                                                                           |
| BFNIH       | BORDER FORCE NATIONAL INTELLIGENCE HUB                                                              |
| CJSM        | CRIMINAL JUSTICE SECURE MAIL                                                                        |
| CMIS        | CHANNEL MANAGEMENT INFORMATION SYSTEM                                                               |
| CRIMINT     | CRIMINAL INTELLIGENCE                                                                               |
| CRIMINT CIS | CRIMINT CRIMINAL INTELLIGENCE SYSTEM                                                                |
| CRIS        | CRIME REPORTING INFORMATION SYSTEM                                                                  |
| CT          | COUNTER-TERRORISM                                                                                   |
| CTCO        | COUNTER-TERRORISM CASE OFFICER                                                                      |
| CTP         | COUNTER-TERRORISM POLICING HEADQUARTERS                                                             |
| DSAB        | DIGITAL SERVICES AT THE BORDER                                                                      |
| DVLA        | DRIVING AND VEHICLE LICENSING AGENCY                                                                |
| ECHR        | EUROPEAN CONVENTION ON HUMAN RIGHTS                                                                 |
| FIMU        | FIXED INTELLIGENCE MANAGEMENT UNIT                                                                  |
| HMRC        | HM REVENUE AND CUSTOMS                                                                              |
| ICO         | INFORMATION COMMISSIONER'S OFFICE                                                                   |
| LEDS        | LAW ENFORCEMENT DATA SERVICE                                                                        |
| LGBTQ+      | LESBIAN, GAY, BISEXUAL, TRANSGENDER AND QUEER, PLUS OTHER SEXUAL ORIENTATIONS AND GENDER IDENTITIES |
| MOPAC       | MAYOR'S OFFICE FOR POLICING AND CRIME                                                               |
| NCA         | NATIONAL CRIME AGENCY                                                                               |
| NPCC        | NATIONAL POLICE CHIEFS' COUNCIL                                                                     |
| PAW         | PORT'S AUTHORITY WATCHLIST                                                                          |
| PCMT        | PREVENT CASE MANAGEMENT TRACKER                                                                     |
| PLP         | POLICE-LED PARTNERSHIP                                                                              |
| PNC         | POLICE NATIONAL COMPUTER                                                                            |
| PND         | POLICE NATIONAL DATABASE                                                                            |
| PSED        | PUBLIC SECTOR EQUALITY DUTY                                                                         |
| QUEST       | QUERYING USING ENHANCED SEARCH TECHNIQUES                                                           |
| RSI         | RIGHTS & SECURITY INTERNATIONAL                                                                     |
| VDOS        | VEHICLE DESCRIPTIVE ONLINE SEARCH                                                                   |
| WI          | WARNINGS INDEX                                                                                      |

# Executive Summary

Prevent, a UK counter-extremism programme that affects thousands of young children and teenagers throughout Great Britain every year, is both a policing and a surveillance programme. Despite Home Office portrayals of the programme as concerned with 'safeguarding', we show that the police are using Prevent referrals as a way to gather 'intelligence' – in fact, Fixed Intelligence Management Units (FIMUs) have primary responsibility for the Prevent process within individual police forces. The government has told us that most people referred to Prevent are never notified of that fact.

While an initial referral – including the referral of a child – will go to the police for storage on their dedicated Prevent databases, this data does not stay under lock and key. In fact, the data ends up on a wide range of police and other databases that the UK government uses for a wide range of purposes, including immigration. And while official policy says the police must usually delete data stored on the designated Prevent database after six years, the data can remain in other databases indefinitely – risking real long-term impacts on the person referred, including children who have since become adults.

This mass data-gathering and sharing on children and others stems from three interrelated practices:

1. Police duplicate records across their databases, meaning that a case initially entered into the specific Prevent databases can end up in other policing databases and used for other policing purposes.
2. Policing databases are automatically synchronised, meaning that once Prevent data is entered into one policing system, it very easily spreads into others.

3. Other government agencies have direct access to policing databases, or some other form of access to records stored on them.

Prevent is also a surveillance programme – one that mainly affects children and teens, and which the government uses to try to change their beliefs. In doing so, the government treats children as unwitting sources of 'intelligence' and relies on policing rather than other potential approaches, such as support for parenting or the ability of teachers to engage in constructive dialogues. Arguably, the programme treats parents as untrustworthy.

Our investigations indicate that Prevent may be primarily affecting children and young people (and, by extension, parents) who are of Asian, Black, Middle Eastern or other minority descent. Other research points to an extensive impact on neurodiverse children. We conclude that it is likely that to a very significant extent, these are the people whom the government – via Prevent – is treating as a source of intelligence and policing information.

Prevent is not a voluntary or consensual programme and data-sharing under it does not take place on the basis of consent. Police automatically share Prevent data with a wide range of other government bodies and ensure that information about a referral is available to other officers as a form of 'intelligence'. All the while, the child or young person referred to the programme – or their parents or caregivers – usually do not realise the referral has happened. Even if they are notified in some manner, the authorities do not tell them about all the places where the police will store or share this data.

The data can include information that is sensitive and may be misleading or false. For example, it may include information about actual or perceived race, religion or belief, opinion, thought, mental health, disability or sexual orientation.

Our research further indicates that Channel – a follow-on stage to Prevent involving more active intervention by police and local authorities – is not voluntary, either, even though the government frequently portrays it that way. Counter-Terrorism Policing (CTP) advises police to provide Channel-style intervention even if the person – usually a child or teen – does not consent to the Channel process, or if the police do not want to ask for their consent. This avoidance of consent is done through a Police-Led Partnership (PLP), which operates in the same way as the Channel process – just without the individual knowing about it. In our view, 'consent' is not consent if the authorities intend to take action regardless.

Our investigation also reveals that the police are willing to 'undermine' the 'status or credibility' of someone referred to Prevent and 'limit their activity', regardless of whether they believe that the person may have broken the law – an approach that treats children like criminal masterminds and raises concerns about potential undercover operations against both children and adults.

Secretly undermining someone's 'status or credibility' is a covert activity of the kind usually undertaken by intelligence agencies, and we conclude that it further erodes the government's claims that Prevent is a 'safeguarding' programme. Such an approach also calls into question whether schools, GPs and others understand the real implications of referring someone to Prevent.

To 'undermine' a person in this way (again, including children and teens, who are the subject of most Prevent referrals), police can use a 'full range' of investigative powers, such as gaining access to 'mobile phone location records' and 'phone data downloads', as well as collecting information about the person's 'online footprint'.

Despite all this hoarding of personal data – including sensitive personal data that should be subject to extra protections under the Human Rights Act 1998 – the government appears to be both unwilling and unable to use that data to assess whether it is operating Prevent in a discriminatory way. In this report, we detail the haphazard and inconsistent storage of data related to protected characteristics such as race, religion, disability and sexual orientation that currently makes it impossible for the police or the Home Office to conduct any fact-based equality assessment. This apparent failure to consider the strategy's equality impacts is occurring despite long-held and often-expressed concerns among academics and civil society groups about potentially racist and Islamophobic patterns in referrals, as well as concerns more recently expressed by parents and others about the potential impact of Prevent on neurodiverse children.

The research we detail below only begins to describe the spider's web of Prevent data. In this report, we focus only on the use and sharing of Prevent-related personal data by the police; however, other public bodies may frequently share and store the data, including in relation to cases that never reach the stage of a formal Prevent referral. Further interrogation of how other public bodies treat Prevent data is needed to fully understand the impact a referral can have on a child's life, or an adult's.

Finally, the government and the police are not acting transparently. Throughout this report, we describe many instances in which government guidance and pronouncements are at best misleading, and at worst plainly incorrect.

Under Article 8 of the European Convention on Human Rights (ECHR), governments are obligated to uphold everyone's right to respect for their private and family life. This duty includes a requirement that laws governing the collection and handling of a person's private information must be clear, accessible, and stipulate the circumstances under which the government or other institutions can process the personal data.<sup>1</sup> By establishing a convoluted spider's web of databases, the UK government has created an environment in which people – such as children and their parents – will have almost no idea where their personal data is stored, what the data includes, whether it is correct, who has access to it and what the consequences could be (if those people are even notified of the Prevent referral in the first place, which usually will not be the case).

We conclude that this situation breaches Article 8 as well as related rights such as the freedoms of expression, religion and association; it may also violate the specific rights of people with disabilities.

Prevent is a programme that directly impacts thousands of people in Great Britain, most of them children, every year. That means the scale of these harms and potential harms is serious and deserves attention from the UK government at the highest levels. It is not acceptable under international law to ignore a known problem that harms thousands of children annually.

A note about language: In this report, we occasionally refer to 'children and teenagers'. Under international standards and UK law, the age of majority is 18, meaning that anyone under 18 is a child. Our phrasing reflects the government's choice of age categories when reporting on Prevent: historically, the Home Office has used the categories of 'Under 15' and '15-20', meaning that we do not know how many people referred to Prevent during most years of its operation have been children (i.e., under 18). From 2024 onwards, the Home Office provided a more useful breakdown, stating that during the most recent year of reporting (April 2023 to March 2024), 57 percent of Prevent referrals – that is, 3,918 of them – concerned children aged 17 and under. Among those referrals, 297 were for children under 10.<sup>2</sup>

---

<sup>1</sup>For further discussion on the UK's obligations under Article 8 in relation to data collection see, Rights & Security International, '[Secret, Confused and Illegal: How the UK Handles Personal Data Under Prevent](#)' (2022), pp. 37-47.

<sup>2</sup>Home Office, '[Individuals referred to and supported through the Prevent Programme, April 2023 to March 2024](#)' (5 December 2024), '[data tables](#)', Table 4.

# Who Is Affected by Prevent?

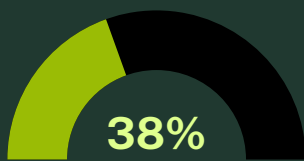
## Mostly children and teens



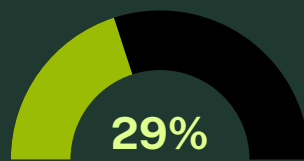
# 63%

In the year ending 31 March 2023, there were 6,817 referrals to Prevent. **63% of all Prevent referrals are for individuals under the age of 20.**

## Primary referral sources



Education sector



Police

Since 2015/16, the Education sector has consistently contributed a third (33%) of all referrals, now up to 39% in 2023.

## Age breakdown

15-20 years old 32%

14 years old and below 31%

Of the referrals where age of the individual was known (6,796), those aged 15 to 20 again accounted for the largest proportion (2,203; 32%). Those aged 14 years and under account for the second largest proportion (2,119; 31%) of referrals.

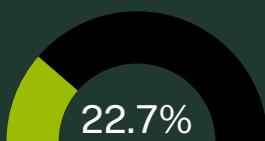
## Gender



# 90%

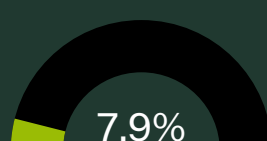
Of cases where gender was specified (6,801), 90% were male (6,125 referrals)

## Prevent Referrals by Racial Demographics



Asian

Although only 9.3% of the general population in England and Wales is Asian



Black

Compared to just 2.5% of the general population



Middle Eastern

Though fewer than 1% of people identified as Arab in the census



White

Despite this group representing 81.7% of the population



# KEY FINDINGS

## Prevent Case Management Tracker (PCMT)

### Data collection

The Prevent Case Management Tracker (PCMT) contains a significant amount of personal data, including information about the person's immigration and employment status, family and other relationships, and their social media activity.<sup>3</sup>

It is not clear which agency is responsible for running the PCMT: the NPCC has told us in correspondence that Counter-Terrorism Policing Headquarters (CTP) 'manages' the PCMT, that the Metropolitan Police 'hosts' the database, and all police chief officers jointly 'control' it.<sup>4</sup> However, both the NPCC and the Home Office have also said that the NPCC and CTP are not legal entities, meaning that it is not clear to us what the nature of these bodies is and whether they could, legally speaking, 'manage' or 'control' anything.<sup>5</sup> We also do not know what the NPCC means by 'hosts', 'manages' or 'controls'.

The collection and storage of information related to a person's immigration status sets the stage for police and government data-sharing for immigration purposes, even though Prevent is not supposed to be about determining or trying to revoke someone's immigration status.<sup>6</sup>

Similarly, the collection and storage of employment data sets the stage for the police sharing information about a person's political or religious views (or perceived views) with their employer without their consent.<sup>7</sup>

The police, through their 'model' Prevent form, advise Prevent practitioners not to seek consent to the collection and sharing of vast quantities of personal data when they refer someone to Prevent.<sup>8</sup>

### Collection and use of data on racial identity

Both the police and the Home Office are unable (and, we argue, unwilling) to carry out a fact-based assessment of whether the Prevent referral system is having discriminatory impacts.<sup>9</sup>

Despite well-known risks of Prevent's disproportionate impact on people who identify as Black, Asian or of Middle Eastern descent (or who are perceived that way), neither the Home Office nor the police are collecting data in a way that would allow them to assess whether Prevent is having a discriminatory impact. The data they collect, as they have admitted to us in correspondence, is too low in quality to make such an assessment possible.

<sup>3</sup>See Counter Terrorism Policing Headquarters, 'Policy for Prevent Practitioners: Management of CT/DE Risk within the Community', June 2018, Section Four; Metropolitan Police, , June 2018, Section Four; Metropolitan Police, 'Freedom of information request reference no: 01.FOI.20.20.015862', no date., no date.

<sup>4</sup>Metropolitan Police, communication with RSI, ref no. 202558/KXP, 9 August 2024, paras. 3-5.

<sup>5</sup>Government Legal Department, communication with RSI on behalf of the Home Office, ref no. Z2409530/CB4/DS4, 17 September 2024, para. 3; Metropolitan Police, communication with RSI, ref no. 202558/KXP, 9 August 2024, para. 2.

<sup>6</sup>For more information, see Home Office, '[National Law Enforcement Data Programme Law Enforcement Data Service \(LEDS\) – Privacy Impact Assessment Report](#)' (July 2018), para. 4.5.

<sup>7</sup>See e.g. Counter Terrorism Policing, '[Purpose Specific Data Sharing Agreement \(DSA\) Between SO15 Local Operations And Lewisham Local Authority](#)', CTP-CA-132 (22 September 2020), p. 6

<sup>8</sup>See Annexes A and B.

<sup>9</sup>See Annexes F-O



# KEY FINDINGS

While the police and the Home Office collect some data on the perceived racial identity of people referred to Prevent, they tell us that they do not do so for statistical or equality monitoring purposes, and they do not do it consistently. In fact, racial identity data (which is based on the perception of the referrer, rather than being self-reported) is only recorded for a relatively small minority of Prevent cases. In the majority of cases, race is not recorded at all, or is recorded as 'unknown'. Figures we have obtained from the government indicate that this trend of missing race data that could have enabled equality monitoring is worsening.<sup>10</sup>

Instead, the government has told us that it collects racial identity data only sometimes, when it thinks the data could be 'relevant' to the referral. The government has not told us anything further about when and why its Prevent policy-makers think race per se would be relevant to understanding whether someone might engage in violence, or how it avoids what appears to us to be an obvious risk: that Prevent referrers will record an individual's race mainly when the referrers are being influenced by racist stereotypes.<sup>11</sup>

The Home Office and the police told us explicitly that their data regarding the racial identity of people referred to Prevent is likely inaccurate, in part because they do not rely on the individual's description of their own racial identity, instead relying on the referrer's perception.<sup>12</sup>

The Home Office and the police take a different approach to recording the racial identity of people impacted by Prevent in comparison with their racial impact assessments for other policing and counter-terrorism activities. Both bodies use an '18+1' model – that is, a list of 18 racial/ethnic categories plus an option for 'unknown' – to monitor the impact of other policing and counter-terrorism programmes, but not when they are monitoring the impact of Prevent, when they use only five categories (plus 'unknown').<sup>13</sup> This inconsistent and broad approach is a factor in the government's inability to discover and monitor any discriminatory impacts of the Prevent strategy.

## Data collection

The Home Office and the police take a different approach to recording the racial identity of people impacted by Prevent in comparison with their racial impact assessments for other policing and counter-terrorism activities. Both bodies use an '18+1' model – that is, a list of 18 racial/ethnic categories plus an option for 'unknown' – to monitor the impact of other policing and counter-terrorism programmes, but not when they are monitoring the impact of Prevent, when they use only five categories (plus 'unknown').<sup>13</sup> This inconsistent and broad approach is a factor in the government's inability to discover and monitor any discriminatory impacts of the Prevent strategy.

---

<sup>10</sup>Rights & Security International, '[New data on Prevent raises racism concerns](#)' (Rights & Security International, 1 October 2024); National Police Chiefs' Council, '[Freedom of Information Request Reference Number: 181/2024](#)' (17 June 2024), p. 2.

<sup>11</sup>Zin Derfoufi and Sarah St. Vincent, '[Analysis of FOI 63470 data on the ethnic composition of Channel cases, and a comparison to the composition of terrorism-related criminal sanctions](#)' (Rights & Security International, February 2023); Rights & Security International, '[New data on Prevent raises racism concerns](#)' (Rights & Security International, 1 October 2024).

<sup>12</sup>See Annexes XX, XX...

<sup>13</sup>Zin Derfoufi and Sarah St. Vincent, '[Analysis of FOI 63470 data on the ethnic composition of Channel cases, and a comparison to the composition of terrorism-related criminal sanctions](#)' (Rights & Security International, February 2023), p. 5.

# KEY FINDINGS

## Data input

The PCMT contains much more data than the public or most UK lawmakers likely realise, including information about ‘potential referrals’: that is, records of communications about people, including children, who are never actually referred to Prevent.<sup>14</sup>

The inclusion of ‘potential referrals’ on the PCMT, a policing database where those records could be maintained for years, misleads teachers, doctors and other Prevent practitioners tasked with engaging with the police about such ‘potential referrals’. Meanwhile, the government has incorrectly stated that only formal referrals are recorded on the PCMT.<sup>15</sup>

## Prevent as intelligence: The role of FIMUs

The PCMT process is secretly run by police intelligence teams within local police forces. Fixed Intelligence Management Units (FIMUs) have a central but poorly understood role throughout the Prevent decision-making process.<sup>16</sup>

FIMUs are also tasked with ‘disrupting’ people referred to Prevent. They are also tasked with ‘undermining’ the ‘status/credibility’ of people referred to Prevent and ‘limit[ing] their activity’.<sup>17</sup>

It is unclear what each of these terms mean in this context, but any attempt to interfere with people’s – especially children’s – lives based on what those people might think, especially when there is no indication that they plan to engage in violence, would raise human rights concerns. Secret surveillance or covert operations, such as a covert effort to embarrass or humiliate someone, would have even greater implications for human rights.

The centrality of FIMUs in Prevent decision-making shows Prevent for what it really is: an intelligence programme, and one directed mainly at children and teenagers.

## Progressing a referral to a Channel panel

When the police progress a case to a Channel panel, this decision gives a wide range of public and private bodies access to that individual’s personal data; these bodies can then store that data on their own internal databases.<sup>18</sup> For example, local police forces, hospitals and other healthcare providers, or schools.

<sup>14</sup>Metropolitan Police, ‘Freedom of information request reference no: 01.FOI.20.20.015862’, no date; Counter Terrorism Policing Headquarters, *The Counter-Terrorism Case Officer Guide* (7 December 2020), p. 30.

<sup>15</sup>Home Office, *Individuals referred to and supported through the Prevent Programme, April 2023 to March 2024* (5 December 2024), section 1.3.

<sup>16</sup>Counter Terrorism Policing, *Secure Systems Administrator – Fixed Intelligence Management Unit – Police Staff – Counter Terrorism Policing NW* (Counter Terrorism Policing, no date); British Transport Police, *Fixed Intelligence Management Unit (FIMU) Officer* (British Transport Police, no date); Document Number NCTPHQ/ICT/218 QRG, 30 May 2018; Metropolitan Police, ‘Freedom of information request reference no: 01.FOI.20.20.015862’, no date; Jason Hogg, *Preventing Future Deaths response of the Chief Constable of Thames Valley Police*, letter to The Rt Hon Sir Adrian Fulford PC KC, 15 July 2024; Suffolk Multi Agency Safeguarding Hub, *Standard Operating Procedures*, v6, July 2022; Lancashire Constabulary, *CTPNW 003-24 Intelligence Management Unit – Detective Sergeant* (Tal.net, October 2024); Bedfordshire Police, *ERSOU – Counter Terrorism – Prevent Sergeant / Staff Supervisor (PO1) – 11286* (Tal.net, November 2022).

<sup>17</sup>Home Office, *Revised Prevent duty guidance: for England and Wales (2015)*, 7 May 2024. See, e.g. Bedfordshire Police, *ERSOU – Counter Terrorism – Prevent Sergeant / Staff Supervisor (PO1) – 11286* (Tal.net, November 2022); Counter Terrorism Policing Headquarters, *The Counter-Terrorism Case Officer Guide* (7 December 2020), pp. 81-82.

<sup>18</sup>See Figure XX below.

# KEY FINDINGS

## Progressing a referral to a Channel panel

When the police do not want to seek an individual's consent to the Channel process, or if the person has refused to consent, then the police instead may effectively continue with the Channel process without telling the person involved. Instead, the police will create what the government calls a Police-Led Partnership (PLP).<sup>19</sup>

As with Channel, when the police create a PLP, this decision allows a wide range of public and private bodies to get access to sensitive personal data about the individual, without the person knowing. The entities that could gain access to the person's data include, for example, the National Crime Agency.<sup>20</sup>

There is an additional risk that the police will send PLP data to foreign law enforcement agencies, through the involvement of the National Crime Agency.<sup>21</sup> This means, for example, that the UK authorities could send data about a child from Iran to the Iranian police.

## Prevent as policing: Extending the 'spider's web'

The police duplicate PCMT records and copy them into other policing databases that are not related to Prevent, including databases for storing criminal offence data and 'intelligence'.<sup>22</sup>

The police may store Prevent data in these other policing databases for much longer than in the PCMT. If someone refers a child to Prevent when the child is 15, the child's personal data will remain in the Police National Computer (PNC) for another 85 years, while at least in theory, their data would only appear in the PCMT until they turned 21 (assuming that the government did not extend the retention period).

The storage of Prevent data on other policing databases rapidly expands the range of people and public bodies that have access to this data. Entities with access to such data include MI5, MI6, His Majesty's Revenue and Customs (the UK tax authority) and the Charity Commission, which regulates nonprofits.<sup>23</sup>

The Home Office also has access to Prevent data contained within these policing databases, and it searches these databases when making decisions about somebody's application for naturalisation as a British citizen. A Prevent referral could therefore impact someone's citizenship.<sup>24</sup>

<sup>19</sup>See CTP, 'CTP-Prevent Policy 2020 Prevent Case Management by CTCOs & CTCO Supervisors' (6 November 2021), p. 28; CTP, The Counter-Terrorism Case Officer Guide (7 December 2020), pp. 63-69.

<sup>20</sup>See Figure XX below.

<sup>21</sup>See Figure XX below.

<sup>22</sup>See Figure XX below.

<sup>23</sup>See Figure XX below.

<sup>24</sup>Home Office, 'Nationality: good character requirement' (31 July 2023). See, e.g. MB v. Secretary of State for the Home Department, SN/47/2015, 22 December 2016; Mustafa Ates (MUA) v. Secretary of State for the Home Department, SN/96/2021, 17 January 2023.

# KEY FINDINGS

Local police forces have access to these non-Prevent-related policing databases, and many of them (either automatically or manually) sync records with their national equivalents. Therefore, data about a Prevent referral could end up all over the country.<sup>25</sup>

As a result of this extensive duplication and sharing, Prevent data also ends up in other secretive databases, for example those run by the Ports Authority and the UK Border Force.<sup>26</sup> Such practices lead to significant 'mission creep' and show the even broader potential impact a Prevent referral can have.

---

<sup>25</sup>E.g. Datalynx, the company that assisted all UK police forces in accessing the Police National Database, said that it created the '[a]utomated [s]haring of [i]ntelligence': Datalynx, 'Police National Database' (Datalynx, no date).

<sup>26</sup>See Figure XX below.

# Introduction: What is Prevent and whom does it affect?

In December 2023, an eight-year-old British-Palestinian boy in London wore a coat with a Palestinian flag stitched onto it. He had friends and family who had been killed by Israeli forces in Gaza, and wanted to honour their memory while showing his identity.

Expressing their identity at school is something children do every day. However, rather than letting the child show his identity and honour his lost friends and family – just as they would presumably do for most children grieving the loss of loved ones – the school decided to do the opposite: it threatened the child's parents with a Prevent referral. The school also threatened other parents who supported the child with a Prevent referral.<sup>27</sup>

While concerns about government, school and police and crackdowns on pro-Palestinian solidarity movements have grown since the outbreak of the Israel-Hamas conflict in October 2023, the problem of Prevent referrals and threatened Prevent referrals affecting children who are expressing their identity are not new.<sup>28</sup>

The pupil actually said 'alms for the oppressed', an expression of their religious identity and education, but the school appears to have coupled this misunderstanding with biased views of the pupil and their perceived identity, referring the child to the counter-terrorism police.<sup>29</sup>

Famously among organisations and families concerned about Prevent, a similar episode of misunderstanding and stereotyping had occurred in 2016 when a nursery referred a four-year-old Muslim-identifying boy to Prevent after misreading his writing – confusing 'cucumber' for 'cooker bomb'.<sup>30</sup>

The UK government's stated purpose for operating Prevent is to stop people from being drawn into terrorism, mainly by detecting people who may hold what the government regards as 'extremist' beliefs. A referral to Prevent does not require someone to have expressed any particular opinion, belief or intention; instead, a teacher, doctor, nurse, social worker, someone working for some other public body, or a member of the public can make a referral based on a guess about what the person might think. (In the UK, the main health system is state-run, meaning that most medical care providers are effectively part of public bodies.) No evidence is required, and the person in question might never have said or written anything relevant.

The Prevent process has three stages: the initial referral, Prevent, and (potentially) the follow-on programme called Channel. In this report, we identify concerns with data collection, storage and sharing across each of these three parts of the Prevent process.

---

<sup>27</sup>For more information, see Claire Hymer, 'British-Palestinian Boy 'Humiliated' By School for Wearing Flag' (Novara, 21 December 2023); Richard Adams, 'East London school in Palestinian flag row could close after threats and abuse' (The Guardian, 19 January 2024).

<sup>28</sup>Rights & Security International, 'Israel-Hamas conflict: Increased police presence in UK schools risks discouraging children's lawful, peaceful speech' (Rights & Security International, 2 November 2023).

<sup>29</sup>For more information, see Diane Taylor, 'Boy, 11, referred to Prevent for wanting to give 'alms to the oppressed'' (The Guardian, 27 June 2021).

<sup>30</sup>See BBC News, 'Radicalisation fear over cucumber drawing by boy, 4' (BBC News, 11 March 2016).

The formal Prevent process starts when a public body refers an individual to the police, often using the 'model' Prevent referral form (see Annexes A and B). (Private individuals such as family members may make Prevent referrals, but the overwhelming majority of referrals are from state-run bodies or other institutions, such as universities.) Referrals generally come from public bodies subject to the 'Prevent duty', which is the statutory obligation to have 'due regard to the need to prevent people from being drawn into terrorism'.<sup>31</sup> Authorities subject to the Prevent duty include schools, hospitals and local councils.<sup>32</sup> In the year ending 31 March 2024 (the most recent year for which data is publicly available), 40 percent of referrals came from the education sector, 28 percent came from the police, and 10 percent came from healthcare providers.<sup>33</sup>

Once the police receive a referral, they will assess how to proceed with the case. Many Prevent cases stop here, as the police decide to mark them as requiring 'no further action' (19 percent), or transfer them to other services, such as health and social care providers (65 percent).<sup>34</sup> In other words, in about 84 percent of all Prevent cases, the authorities appear to decide there is little or no risk of violence against others.

Around 13 percent of referrals progress to a Channel panel – a body consisting of education providers, social workers, mental health professionals, and others, depending on the individual's circumstances – which meets periodically to discuss the individual's situation and provide them with the 'support' needed to address or change their 'ideology'.<sup>35</sup>

However, not all cases that the police refer to Channel end up as Channel cases. Only 58 percent of cases that the police referred to Channel were adopted by a Channel panel in the year ending 31 March 2023. The remaining cases were either left for no further action, signposted to other services, or may instead have been recreated as a 'Police-Led Partnership' (PLP) – a secret alternative to Channel.

There are several groups of people that are, or appear to be, more likely to be subject to a Prevent referral and/or Channel intervention. The relatively well-known cases mentioned above have three things in common: they involve (1) a child (2) who is Muslim or perceived as Muslim, and (3) who is or is perceived to be a member of a racial group that is a minority in the UK (for example, Asian, Black or Middle Eastern – to use the Home Office's terms). While there are many reasons to be cautious about treating those cases as representative of the whole, there are also statistical and other reasons to believe they reflect real trends in Prevent referrals (or threats of referrals).

The police and the government have long targeted British Muslims and Muslim communities in their counter-terrorism and counter-extremism interventions.<sup>36</sup> (Indeed, under the government's first iteration of Prevent, it focused its counter-extremism work only on Muslim communities.)<sup>37</sup> Cases involving suspected 'Islamist extremism' continue to make up a significant percentage of Prevent cases.<sup>38</sup>

---

<sup>31</sup>Counter-Terrorism and Security Act 2015, s26(1).

<sup>32</sup>Counter-Terrorism and Security Act 2015, s26(2). For a list of public bodies subject to the duty, see Schedule 6.

<sup>33</sup>Home Office, 'Individuals referred to and supported through the Prevent Programme, April 2023 to March 2024' (5 December 2024), Figure 2.

<sup>34</sup>Home Office, 'Individuals referred to and supported through the Prevent Programme, April 2023 to March 2024' (5 December 2024), Figure 2.

<sup>35</sup>HM Government, 'Channel duty guidance: Protecting people susceptible to radicalisation: Guidance for Channel panel members' (2023).

<sup>36</sup>[1] See, e.g., Madeline Sophie Abbas, 'Producing 'internal suspect bodies': divisive effects of UK counter-terrorism measures on Muslim communities in Leeds and Bradford' (2019) 70(1) British Journal of Sociology 261.

<sup>37</sup>For an explanation, see Paul Thomas, 'Changing experiences of responsabilisation and contestation within counter-terrorism policies: the British Prevent experience' (2017) 45(3) Policy and Politics 305.

<sup>38</sup>Home Office, 'Individuals referred to and supported through the Prevent Programme, April 2023 to March 2024' (5 December 2024), section 4.



Meanwhile, although the Home Office does not provide information about the racial identity of people referred to Prevent in its annual statistics release, we have been able to gain access to some of this data through freedom-of-information requests. (We add a caveat here that both the Home Office and the police have told us that the data is likely inaccurate.) As we have previously concluded in an analysis of some of the statistics we received, the data suggests that ‘people recorded as Asian and cases recorded as “Islamist related” were subject to comparatively greater scrutiny than other ethnic groups and type of concern’ under Prevent and Channel, and that ‘[b]y contrast, cases involving “right wing extremism”, which primarily involve people recorded as white, [are] increasingly referred to other services or designated as requiring no further action.’<sup>39</sup>

The highly incomplete figures we received about the race of people referred to Prevent from 2019 to early 2024 also suggest that in England and Wales, people recorded as being Black, Asian or Middle Eastern may be experiencing Prevent referrals at rates vastly disproportionate to their share of the population.<sup>40</sup>

Prevent is also a children’s rights issue. With 40 percent of all referrals coming from the education sector and 57 percent involving children younger than 18 years old, Prevent disproportionately impacts children and teenagers. (Children also account for 59 percent of all Channel cases.)<sup>41</sup> In particular, Prevent disproportionately impacts boys, with 88 percent of Prevent referrals and 91 percent of cases discussed at a Channel panel involving people identifying as male.

(The Home Office notes that some of its data may be inaccurate and that it does not have information about the gender identity of everybody referred to Prevent.)<sup>42</sup>

Prevent also significantly impacts neurodivergent people, with a recent investigation by the Financial Times uncovering the existence Home-Office-commissioned research on a potential overrepresentation of autistic people in Prevent. This research – which has never been published and which RSI has not seen – reportedly indicates that approximately one quarter of people receiving Channel interventions have been diagnosed with autism spectrum disorder.<sup>43</sup>

The government regularly refers to Prevent as a ‘safeguarding’ strategy – for example, in explaining the Prevent duty to people working at public bodies, the government states that ‘Prevent sits alongside long-established safeguarding duties on professionals to protect people from a range of other harms’.<sup>44</sup>

As Prevent referrals generally do not respond to clear threats of violence and seldom result in violence-related interventions, and as the programme also is not designed to detect abuse or exploitation as such, we conclude that it is not in fact a ‘safeguarding’ scheme for either the people referred to it or the general public. In our work, RSI has also encountered (for example) at least one instance of children and parents who were threatened in writing with referrals to Prevent as a way of deterring political speech in local schools, and we note that if Prevent were truly a ‘safeguarding’ scheme, it would make little sense to use it as a basis for threats.

---

<sup>39</sup>Zin Derfoufi and Sarah St. Vincent, ‘[Analysis of FOI 63470 data on the ethnic composition of Channel cases, and a comparison to the composition of terrorism-related criminal sanctions](#)’ (Rights & Security International, February 2023), p. 2. This analysis is based on data from 2015/16 to 2018/19, as subsequent data was not available at the time.

<sup>40</sup>See Rights & Security International, ‘[New data on Prevent raises racism concerns](#)’ (Rights & Security International, 1 October 2024).

<sup>41</sup>Home Office, ‘[Individuals referred to and supported through the Prevent Programme, April 2023 to March 2024](#)’ (5 December 2024), ‘[data tables](#)’, Table 4. See also Home Office, ‘[Individuals referred to and supported through the Prevent Programme, April 2023 to March 2024](#)’ (5 December 2024), section 3.1.

<sup>42</sup>Home Office, ‘[Individuals referred to and supported through the Prevent Programme, April 2023 to March 2024](#)’ (5 December 2024), ‘[data tables](#)’, Table 5.

<sup>43</sup>Helen Warrell, ‘[Weaponised autism and the extremism threat facing children](#)’ (Financial Times, 18 October 2024).

<sup>44</sup>HM Government, ‘[Prevent duty training: Learn how to support people susceptible to radicalisation](#)’ (Gov.uk, no date).



The government also regularly depicts Prevent as well as its follow-on programme, Channel, as voluntary. However, we show in this report that this is not the case.

The police have a central role in the collection, storage and sharing of Prevent-related data, duplicating it from Prevent-specific databases to other policing systems and sharing it with a range of public- and private-sector partners, including the immigration authorities. Due to police action, Prevent data ends up being stored in a spider's web of databases and systems, potentially impacting an individual's engagement with essential public services such as health and social care.

But this spider's web of Prevent data does not only impact people who have been referred to the strategy – it also has implications for 'potential referrals'. 'Potential referrals' are cases in which a public-sector worker or a member of the public has approached the police for advice about somebody they know, but this has not led to a referral. In these cases, police still store data about the person (including a child) in policing databases.

But this spider's web of Prevent data does not only impact people who have been referred to the strategy – it also has implications for 'potential referrals'. 'Potential referrals' are cases in which a public-sector worker or a member of the public has approached the police for advice about somebody they know, but this has not led to a referral. In these cases, police still store data about the person (including a child) in policing databases.

Our investigation – described below – shows that in reality, Prevent is a largely secret policing and surveillance scheme aimed at people who may hold views that are outside the mainstream or with which the government disagrees. For instance, official Counter-Terrorism Policing (CTP) guidance refers to 'aggravated activists' as a category of people who could require intervention under Prevent.<sup>45</sup>

The programmes are also not voluntary, and they result in a variety of government agencies having access to sensitive information about people's (i.e. overwhelmingly children's and young people's) real or perceived race, religion, health, family situation, and beliefs or opinions.

The way the police and other government agencies hold data under Prevent could have particular long-term implications for young people. Data from the Home Office indicates that during the reporting year 2023-2024, 66 percent of all referrals were of people 21 years old or younger, with 44 percent aged 15 or under; among all referrals, the largest number come from the education sector (40 percent).<sup>46</sup> Through Prevent, the authorities in Great Britain therefore pull thousands of young people into interactions with the criminal justice system, even though they have not committed any offence.<sup>47</sup>

Data retention and sharing under Prevent can have tangible impacts on the lives of children, young people and others. In *R (II) v. Commissioner of Police of the Metropolis*, a case involving a child referred to Prevent, Justice Steyn observed:

---

<sup>45</sup>Counter Terrorism Policing Headquarters, *The Counter-Terrorism Case Officer Guide* (7 December 2020), p. 123.

<sup>46</sup>Home Office, *Individuals referred to and supported through the Prevent Programme, April 2023 to March 2024* (5 December 2024), 'data tables', Table 4.

<sup>47</sup>John Holmwood and Layla Aitlhadj, *The People's Review of Prevent* (February 2022), p.99.

*[A]s long as the Claimant's personal data is retained, he will continue to fear that it may be disclosed to third parties, particularly universities to which he may apply or from which he may receive offers. The "consequences of being tagged as a supporter of terrorism" could be "devastating for individuals and their families". There is no guarantee that the Claimant's personal data will not be disclosed to third parties. Retaining such personal data engenders fear in that young person that they may be tagged (wrongly) as a supporter of terrorism.*<sup>48</sup>

This report expands on our 2022 report *Secret, Confused and Illegal*, in which we analysed the Prevent strategy in light of the right to privacy under the European Convention on Human Rights (ECHR) and UK data protection legislation.<sup>49</sup>

In that report, we concluded, based on available government policies and guidance, that data-storing and processing practices under Prevent are not based on sufficiently clear laws and regulations to meet a requirement under the ECHR that such handling of data must be based on clear, publicly available laws that are specific enough to allow people to understand when and why the government might collect and use their personal information.<sup>50</sup>

We gathered most of the new information that appears in this report by making freedom-of-information requests to government entities. At every stage of the process, the public bodies from which we sought information (the Home Office, the National Police Chiefs' Council or 'NPCC', and the Metropolitan Police) showed a reluctance to provide us with the information we had requested.

This process led us to complain to the Information Commissioner's Office (ICO) about the handling of our requests, including a 'merry-go-round' process we experienced as each body told us that another was the most appropriate recipient for our request, delaying the research process by several months.<sup>51</sup>

As both this report and *Secret, Confused and Illegal* show, the government's uncertainty and lack of transparency about where Prevent data is held, and who is responsible for it, is reminiscent of the broader haphazard and secretive approach to Prevent data.

We have supplemented the information we gained from the freedom-of-information process by reviewing government documents and responses to other people's or organisations' freedom-of-information requests that provide more information about the ways each of the databases works.

---

<sup>48</sup>R (on the application of II) (by his mother and litigation friend, LK) v. Commissioner of Police of the Metropolis [2020] EWHC 2528 (Admin), paras. 77-78.

<sup>49</sup>Rights & Security International, '*Secret, Confused and Illegal: How the UK Handles Personal Data Under Prevent*' (2022).

<sup>50</sup>Open Rights Group, '*Prevent and the Pre-Crime State: How Unaccountable Data Sharing is Harming a Generation*' (2024).

<sup>51</sup>The ICO dismissed RSI's complaint without looking into the wider process of our freedom-of-information request: Information Commissioner's Office, *Decision Notice IC-262164-Z2K6*, 20 December 2023.

# How do the police store data about children and other people under Prevent? And who has access to it?

Although the government defines Prevent as a ‘consensual’ process,<sup>52</sup> in reality it is far from being voluntary or consent-based. In fact, in correspondence with RSI, the Government Legal Department (on behalf of the Home Office) told us that ‘persons referred to Prevent are not generally made aware of their referral unless they are invited to participate in the Channel programme’.<sup>53</sup> This statement contradicts other government pronouncements, although it is consistent with what our other knowledge of Prevent would suggest.

Further, throughout all stages of the referral process, there are many children and other people whose personal information is stored in policing systems without them knowing about it – all while the police are marking them as potential ‘extremists’ or ‘terrorists’ who might intend to cause serious harm to others.<sup>54</sup>

For example, before the referral stage, a teacher may raise concerns to their supervisor that one of their students seems to need a Prevent intervention; however, the designated Prevent lead at the school often decides that a Prevent intervention is not necessary. In these instances, although the school has decided not to refer the child’s case to the police, it will usually retain that information in its local databases in case the information becomes ‘relevant’ in the future.<sup>55</sup>

As we discuss below, this information can also end up in police databases later, for example if the Prevent lead speaks to the police to get their advice on how to proceed. At this point, the child and their family would likely not be aware that the child has been subjected to Prevent-related monitoring.

If the school’s or other public body’s Prevent lead decides to refer a case to the police for Prevent intervention, the government describes this as a consensual process. Such a description might make it sound as if the public body will discuss the concerns it has identified with the individual (or their parents or caregiver) and seek their consent before initiating a referral.<sup>56</sup> However, as we have detailed in *Secret, Confused and Illegal*, the government advises Prevent practitioners to refer people to the programme without seeking their consent, or – as appropriate – the consent of their parents.<sup>57</sup>

We have also identified a failure to seek consent to intervention later in the process, when the police decide whether to launch the much more detailed Channel process. Even if the police decide that a case requires Channel intervention, this decision does not necessarily mean that the police or referring body will tell the person (or their guardians) about the referral and intervention process.

---

<sup>52</sup>As is particularly the case with the Channel process. See e.g. Home Office, ‘[Prevent duty guidance: for England and Wales](#)’ (6 March 2024), paras. 52-56.

<sup>53</sup>Government Legal Department, communication with RSI on behalf of the Home Office, ref no. Z2409530/CB4/DS4, 17 September 2024, para. 5.

<sup>54</sup>For an overview, see Rights & Security International, ‘[Secret, Confused and Illegal: How the UK Handles Personal Data Under Prevent](#)’ (2022), in particular paras. 31-35.

<sup>55</sup>See the Metropolitan Police’s arguments in *R (on the application of II (by his mother and Litigation Friend, NK)) v. Commissioner of Police for the Metropolis* [2020] EWHC 2528 (Admin), paras. 56-73.

<sup>56</sup>For example, see the ‘notice, check, share’ process that official government training explains: Home Office, ‘[Get help for radicalisation concerns](#)’ (Gov.uk, 6 March 2024). Sometimes public bodies reference the consensual nature of a referral, albeit not in all instances: see City of Bradford Metropolitan District Council, ‘[Notice, Check, Share: Questions to Consider](#)’ (no date), p. 2; Kirklees Prevent, ‘[Notice, Check, Share](#)’ (no date). However, some public bodies’ guidance does not reference consent: see Stafford Borough Council, ‘[Our Prevent Strategy](#)’ (11 July 2023); Child Friendly Leeds ‘[One minute guide: No. 102, Radicalisation and preventing extremism](#)’ (October 2020).

<sup>57</sup>Rights & Security International, ‘[Secret, Confused and Illegal: How the UK Handles Personal Data Under Prevent](#)’ (2022), paras. 31-35, 51-61.

For instance, as we explain below, the police can decide under current policy to leave Channel aside and instead turn the case into a Police-Led Partnership (PLP) if officers do not feel it is 'appropriate' to seek the individual's consent for an intervention.

Additionally, our research indicates that the police do not tell the individual affected (or their parents or guardians) when officers replicate or transfer that person's data to other public or private bodies, or when they decide to copy the details of a referral into other police databases.

The result is a secretive spider's web about people – often children – who usually are not suspected of any crime: data about a referral can start off with a school, go through various national and local police forces, and then out to the UK border police and immigration authorities, child welfare authorities and/or the intelligence agencies, all while the referred person and their family are completely unaware.

Our research also calls into question another government assertion about Prevent: that it is not a policing programme.<sup>58</sup>

While two of the databases we discuss here are overtly dedicated to implementing the Prevent strategy (the Prevent Case Management Tracker, or 'PCMT', and the now-redundant Channel Management Information System, 'CMIS'), Prevent data also winds up in other policing databases. At least two of these are databases whose sole purpose is policing: the Police National Computer (PNC) and the CRIMINT Criminal Intelligence System.

In fact, we found a complaint among police about having to re-enter data into multiple databases.

In other words, police have access to the data, including through databases that are only intended for law enforcement. These flows of data through multiple police databases indicate that Prevent is a policing programme: if your child is referred to Prevent, whether through a school, GP surgery or social worker, then the police will hold records about your child, and potentially you as well.

Under UK data protection law, children have some authority to consent to the processing of their personal data. In contrast to the approach data protection law takes to children accessing online services (for which children under the age of 13 cannot lawfully consent),<sup>60</sup> the approach for other forms of data processing and sharing depends on whether the child has the mental capacity to provide their consent.<sup>61</sup> It is unclear to us how the police decide whether to approach the child or their parents to ask for consent to the sharing, storage or other processing of their Prevent-related data: the Home Office's and the Metropolitan Police's data privacy notices do not address this.<sup>62</sup>

There are also non-policing databases where Prevent-related data can be found, as the UK charity Open Rights Group discusses in its 2024 report, *Prevent and the Pre-Crime State*.<sup>63</sup>

Various government bodies and other entities have created different policies for how to treat Prevent data within the databases they manage, and this means that when records are deleted

---

<sup>58</sup>The government and the police claim that it is not a policing programme, but rather is government-led and takes a 'multi-agency' approach, to which the police contribute: see Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services, '[Counter-terrorism policing: An inspection of the police's contribution to the government's Prevent programme](#)' (2020), p. 1. In Scotland, in which the police operate Prevent independently from the approach in England and Wales, see Police Scotland, '[Prevent Referral data](#)' (Police Scotland, no date).

<sup>59</sup>CoPaCC and Policinginsight, '[Police ICT user perspectives: 2018](#)' (2018), pp. 10-11, 36.

<sup>60</sup>See [UK General Data Protection Regulation](#), Article 8.

<sup>61</sup>For a summary, see ICO, '[Children and the UK GDPR](#)' (ICO, no date).

<sup>62</sup>Home Office, '[Channel data privacy information notice](#)' (Gov.uk, 1 August 2024);

<sup>63</sup>Open Rights Group, '[Prevent and the Pre-Crime State: How Unaccountable Data Sharing is Harming a Generation](#)' (2024). The report maps some further information about data flows during the referral process.

from one database, they may continue to exist on others and continue to be used for surveillance purposes – causing further long-term consequences for the child, older teen or adult.

We have also found concerning sources indicating the police are willing to ‘disrupt’ people who hold (or supposedly hold) controversial views, and ‘undermine [a person referred to Prevent’s]... status/credibility and limit their activity’, regardless of whether they believe the person may have committed any criminal offence.<sup>64</sup> In doing so, Prevent practitioners in police forces can use a ‘full range’ of investigative powers, including by gaining access to previously obtained cell-site records and phone data downloads, as well as collecting information about the person’s ‘online footprint’.<sup>65</sup>

Even though Prevent referrals overwhelmingly involve children and older teenagers, and even though those children and young people are regularly referred to Prevent even though there is no evidence that they intend to hurt anyone, the government appears to be legitimising the use of covert human intelligence (i.e. ‘undercover’) operations, as well as intrusive surveillance, to ‘disrupt’ them as if they were the sophisticated leaders of international criminal networks.

The documents we found do not explain what ‘disrupt’ means or appear to place any limits on such ‘disruption’ of children, teens or other people who come to the attention of Prevent.

This broad practice of non-consensual data-hoarding and sharing, and the potential use of Prevent data for ‘intelligence’ and ‘disruption’, indicate that in reality, Prevent is a surveillance programme run by the police.

For a brief summary of each of the databases we discuss, see the table below. Before describing each of these databases in more detail, we note that the government (prior to the 2024 election) agreed to proposals to force more public bodies to comply with the Prevent duty,<sup>66</sup> including immigration authorities and job centres (state agencies that were established help unemployed people in the UK gain access to temporary welfare benefits and employment – although many people perceive them as a barrier to those things in practice).<sup>67</sup> Although our research suggests that immigration authorities may already have access to Prevent-related data, the then-government’s acceptance of these proposals points to a potential expansion of the programme, despite years of critiques on human rights and other grounds. It remains to be seen whether the new government will pursue these policies.

The expansive storage, retention and sharing of Prevent-related personal data can create serious long-term impacts for a person’s life, and the government’s implementation of these new policies would only exacerbate that problem.

---

<sup>64</sup>Home Office, ‘[Revised Prevent duty guidance: for England and Wales \(2015\)](#)’, 7 May 2024. See, e.g. Bedfordshire Police, ‘[ERSOU – Counter Terrorism – Prevent Sergeant / Staff Supervisor \(PO1\) – 11286](#)’ (Tal.net, November 2022).

<sup>65</sup>Counter Terrorism Policing Headquarters, ‘[The Counter-Terrorism Case Officer Guide](#)’ (7 December 2020), pp. 81-82.

<sup>66</sup>This is the obligation to have ‘due regard to the need to prevent people from being drawn into terrorism’ in fulfilling their functions, which ultimately includes obligations to refer people to Prevent: see [Counter-Terrorism and Security Act 2015](#), s26.

<sup>67</sup>William Shawcross CVO, ‘[Independent Review of Prevent](#)’, HC 1072, February 2023, para. 6.9; Home Office, ‘[Independent report: The response to the Independent Review of Prevent](#)’, 13 December 2023, response to Recommendation 8.



# Policing databases where data about people referred to Prevent is held

Figure 1: Policing databases where data about people referred to Prevent is held

| Database                                               | Managing body                                                                                                                                                                      | How long people's data are held                                            | Bodies with access to the data                                                                                                                                                                                                          |
|--------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>The 'old' PCMT-CMIS joint system (pre-May 2024)</b> |                                                                                                                                                                                    |                                                                            |                                                                                                                                                                                                                                         |
| <b>'Old' Prevent Case Management Tracker (PCMT)</b>    | Counter-Terrorism Policing Head Quarters (CTP) <sup>68</sup>                                                                                                                       | 6 years after closure, with a possibility of extension                     | CTP; National Police Chiefs' Council; <sup>69</sup> individual police forces (including counter-terrorism police forces; Home Office; local authorities; other public bodies; private companies                                         |
|                                                        |                                                                                                                                                                                    |                                                                            | If the referral leads to a Policing-Led Partnership (PLP), then other public bodies will have access to PCMT data, including the National Crime Agency, although the PLP decides which bodies will have access on a case-by-case basis. |
| <b>Channel Management Information System (CMIS)</b>    | Home Office (with CTP staff entering data into the database) <sup>70</sup>                                                                                                         | 6 years after the case is removed from the Channel programme <sup>71</sup> | Home Office; CTP; individual police forces; organisations with a 'partnership agreement'                                                                                                                                                |
| <b>The 'new' PCMT system (post-May 2024)</b>           |                                                                                                                                                                                    |                                                                            |                                                                                                                                                                                                                                         |
| <b>'New' PCMT</b>                                      | Home Office and individual Chief Officers for Channel data; CTP (acting on behalf of the Metropolitan Police/Mayor's Office for Policing and Crime (MOPAC)) for other Prevent data | 6 years after closure, with the possibility of extension. <sup>72</sup>    | Same as with the old joint system <sup>73</sup>                                                                                                                                                                                         |

<sup>68</sup>Metropolitan Police, correspondence with RSI, ref no. 202558/KXP, 9 August 2024, para. 3.

<sup>69</sup>The National Police Chiefs' Council, alongside the government, directs CTP: see Counter-Terrorism Policing, '[Counter Terrorism Policing HQ](#)' (no date).

<sup>70</sup>Home Office, '[Channel data privacy information notice](#)' (Gov.uk, 1 August 2024).

<sup>71</sup>Cases are reviewed at 6 months and 12 months after closure of a case. Once the 12-month review has taken place, the 6-year clock begins.

<sup>72</sup>Government Legal Department, communication with RSI on behalf of the Home Office, ref no. Z2409530/CB4/DS4, 17 September 2024, paras. 18-20.

<sup>73</sup>Government Legal Department, communication with RSI on behalf of the Home Office, ref no. Z2409530/CB4/DS4, 17 September 2024, para. 18.

| Other policing databases                                   |                                                 |                                                                                                                                      |                                                                                                                                                                                                                                                                                                            |
|------------------------------------------------------------|-------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Police National Computer (PNC)</b>                      | Home Office;<br>National Police Chiefs' Council | Until the individual's 100th birthday                                                                                                | Individual police forces; Home Office and other government bodies; <sup>74</sup> UK Border Force; independent researchers                                                                                                                                                                                  |
| <b>Police National Database (PND)</b>                      | Home Office;<br>National Police Chiefs' Council | According to policy, generally deleted after six years unless the police believe that the person poses an ongoing risk <sup>75</sup> | Individual police forces; law enforcement agencies; <sup>76</sup> National Crime Agency; a limited number of officers in the Disclosure and Barring Service, Border Force, Immigration Enforcement, Identity and Passport Services, HM Revenue & Customs and the Security Industry Authority <sup>77</sup> |
| <b>CRIMINT Criminal Intelligence Systems (CRIMINT CIS)</b> | Metropolitan Police                             | Potentially indefinitely                                                                                                             | Other policing bodies; Home Office and other public and private bodies                                                                                                                                                                                                                                     |
| <b>Other locally managed policing databases</b>            | Local police forces                             | Varies depending on the database                                                                                                     | Varies depending on the database                                                                                                                                                                                                                                                                           |
| <b>Ports Authority Watchlist (PAW)</b>                     | Unknown                                         | Unknown                                                                                                                              | Individual police forces (through Fixed Intelligence Management Units and Counter-Terrorism Case Officers); Ports Authority; UK Border Force; Counter-Terrorism Policing                                                                                                                                   |
| <b>Warnings Index (WI)</b>                                 | UK Border Force                                 | Unknown                                                                                                                              | Border Force; Immigration Enforcement Regional Intelligence Units; UK Visas and Immigration; <sup>78</sup> other policing bodies; Home Office; <sup>79</sup> other public bodies if shared via a Gateway Multi-Agency Hub                                                                                  |

<sup>74</sup>For a full list, see Unlock, '[Organisations that have access to the Police National Computer \(PNC\)](#)' (Unlock, no date).

<sup>75</sup>For a summary, see Jacqueline Beard, '[The retention and disclosure of criminal records](#)', CBP6441, 17 May 2019).

<sup>76</sup>Datalynx, '[Police National Database, Connecting law enforcement throughout the UK](#)' (Datalynx, no date).

<sup>77</sup>Home Office, '[National Law Enforcement Data Programme Law Enforcement Data Service \(LEDS\) – Privacy Impact Assessment Report](#)' (July 2018), para. 4.5.

<sup>78</sup>Home Office, '[The response to the Parliamentary and Health Service Ombudsman investigation into a complaint by Mrs A and her family about the Home Office](#)' (January 2015), paras. 28, 95 and 115.

<sup>79</sup>Home Office, '[The response to the Parliamentary and Health Service Ombudsman investigation into a complaint by Mrs A and her family about the Home Office](#)' (January 2015), pp. 10, 14, 30-32.



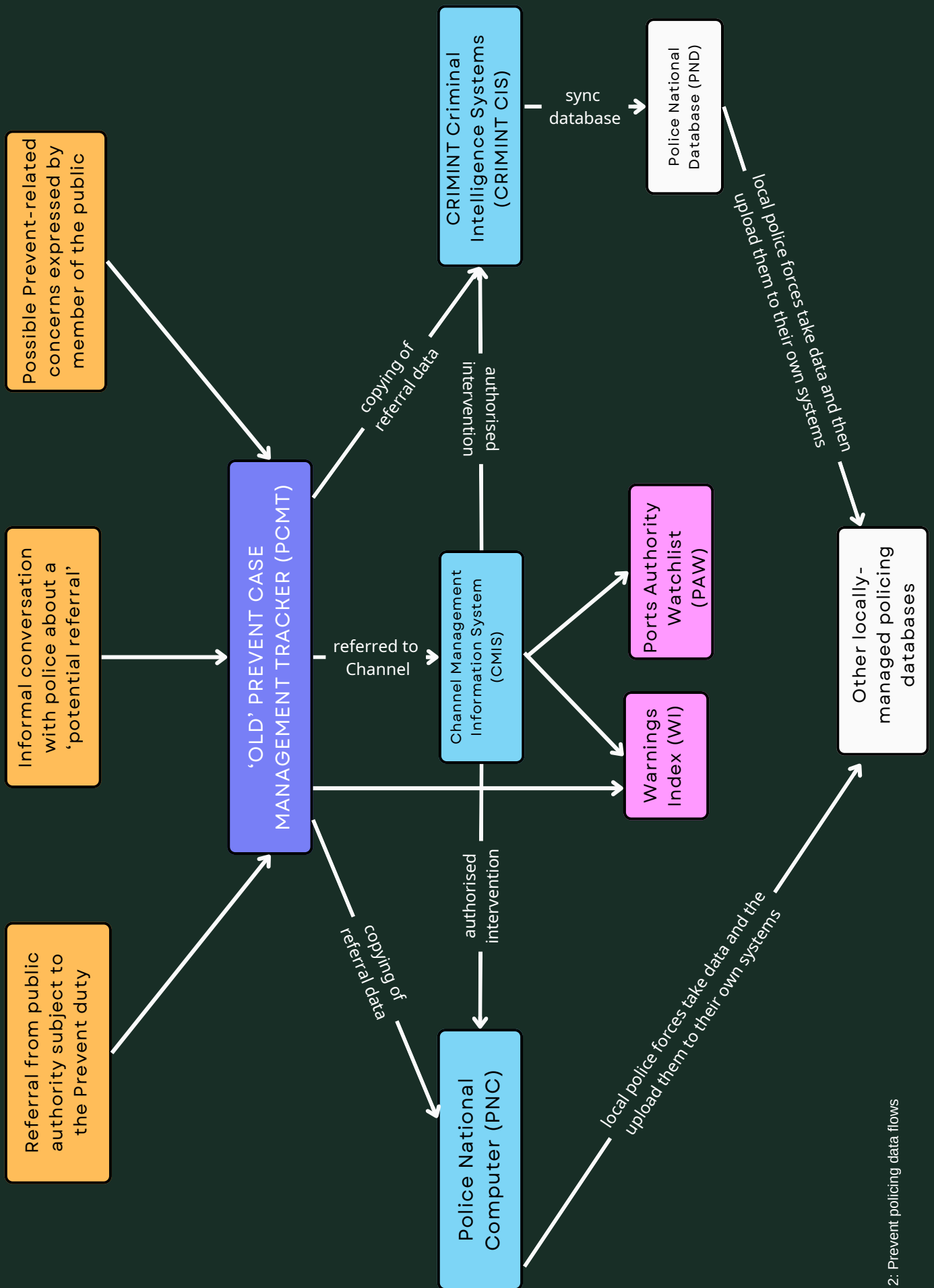


Figure 2: Prevent policing data flows

# Data Sharing Pathways: Who Has Access?

Each icon represents an entity with access to each database



## 'Old' Prevent Case Management Tracker (PCMT)

Managing body:



Bodies with access to data:



Years data is held: **6** years after closure, with a possibility of extension

## 'New' PCMT

Managing bodies:



Home Office



Bodies with access to data:



Years data is held: **6** years after closure, with a possibility of extension

## Police National Database (PND)

Managing bodies:



Home Office



Bodies with access to data:



Years data is held: **6** years unless the police believe that the person poses an ongoing risk

# Data Sharing Pathways: Who Has Access?

## Channel Management Information System (CMIS)

Managing body:



Home Office

Bodies with access to data:

Home Office



COUNTER TERRORISM POLICING

and organisations with a 'partnership agreement'

Years data is held:

6

years after the case is removed from the Channel programme

## Police National Computer (PNC)

Managing bodies:

Home Office



NPCC  
National Police Chiefs' Council

Bodies with access to data:

Home Office



Border Force



Years data is held:

100

Until the individual's 100th birthday

## CRIMINT Criminal Intelligence Systems (CRIMINT CIS)

Managing body:



Metropolitan Police

Bodies with access to data:



Home Office



Years data is held:

Indefinitely

## Other locally managed policing databases

Managing bodies:



Local police forces

Bodies with access to data:

Varies depending on database

Years data is held:

Varies depending on database

## Ports Authority Watchlist (PAW)

Managing bodies: Unknown

Bodies with access to data:



Border Force



COUNTER TERRORISM POLICING

Years data is held:

?

## Warnings Index (WI)

Managing bodies:



Border Force

Bodies with access to data:



Border Force



UK Visas and Immigration



Home Office



Years data is held:

?

Unknown

# The starting point: Prevent Case Management Tracker

## 'Old' Prevent Case Management Tracker (PCMT)

Managing body:



Bodies with access to data:



Years data is held:

6

years after closure, with a possibility of extension

The primary database for Prevent purposes is the Prevent Case Management Tracker (PCMT), which is managed by Counter-Terrorism Policing Headquarters (CTP) and was first used in May 2018.<sup>80</sup> Through this database, police store the personal data of all people (children and adults) referred to Prevent, including people whose cases have been marked as erroneous or as requiring no further action. The police hold this data for at least six years, but in many cases much longer.

In May 2024, the Home Office launched its 'new' PCMT. This new system merges the PCMT with the now-redundant Channel Management Information System (CMIS), a Channel-specific database that had been run by the Home Office; the new, combined system has the stated aim of reducing duplication of records across multiple policing databases and ensuring that all information is up to date. In correspondence with RSI, the Home Office has stated that little has changed about the way in which the police collect Prevent-related data; they assert that the change simply affects how the data is stored.<sup>81</sup>

Throughout this section, we will refer to the PCMT as a whole, encompassing both the 'old' and 'new' systems.

## 'New' PCMT

Managing bodies:



Home Office



acting on behalf of



MOPAC

Bodies with access to data:



Years data is held:

6

years after closure, with a possibility of extension

<sup>80</sup>On the NPCC's role, see Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services, '[Counter-terrorism policing: An inspection of the police's contribution to the government's Prevent programme](#)' (2020). On CTP's role, see Document Number NCTPHQ/ICT/212 QRG, 24 May 2018 and Document Number NCTPHQ/ICT/218 QRG, 30 May 2018. On the PCMT's introduction in May 2018, see Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services, '[Counter-terrorism policing: An inspection of the police's contribution to the government's Prevent programme](#)' (2020), p. 12.

<sup>81</sup>Government Legal Department, communication with RSI on behalf of the Home Office, ref no. Z2409530/CB4/DS4, 17 September 2024, para. 19.

## Data collection

- The Prevent Case Management Tracker (PCMT) contains a significant amount of personal data, including information about the person's immigration and employment status, family and other relationships, and their social media activity.
- It is not clear which agency is responsible for running the PCMT: the NPCC has told us in correspondence that Counter-Terrorism Policing Headquarters (CTP) 'manages' the PCMT, that the Metropolitan Police 'hosts' the database, and all police chief officers jointly 'control' it. However, both the NPCC and the Home Office have also said that the NPCC and CTP are not legal entities, meaning that it is not clear to us what the nature of these bodies is and whether they could, legally speaking, 'manage' or 'control' anything. We also do not know what the NPCC means by 'hosts', 'manages' or 'controls'.
- The collection and storage of information related to a person's immigration status sets the stage for police and government data-sharing for immigration purposes, even though Prevent is not supposed to be about determining or trying to revoke someone's immigration status.
- Similarly, the collection and storage of employment data sets the stage for the police sharing information about a person's political or religious views (or perceived views) with their employer without their consent.
- The police, through their 'model' Prevent form, advise Prevent practitioners not to seek consent to the collection and sharing of vast quantities of personal data when they refer someone to Prevent.

We already know some of the types of data that public bodies collect, process and hold as part of Prevent. Some of this data includes personal information that should have heightened protection under data protection and/or human rights laws. For instance, we can see from the government's annual Prevent statistics that it collects data relating to the referred person's:

- Name;
- Age and date of birth;
- Contact details, including address, phone number and email address;
- Gender identity;
- Opinions and beliefs; and
- Religious views.<sup>82</sup>

The police and the Home Office also store data relating to the referring entity, if that entity is a public body. The collection of data about the referring entity may involve the collection of additional sensitive personal data; for example, if someone is referred to Prevent by their local mental health service, the database may show or suggest that the person has a diagnosed mental health condition.

The government is more secretive about other types of personal information that it captures and

holds under Prevent, which we outline here in further detail. RSI has found this information through various requests under the Freedom of

Information Act 2000, and through access to CTP's model Prevent Referral Form (reproduced in Annexes A and B), in which it advises practitioners about the data they should include as part of a Prevent referral. Although described as a 'model' form, it appears that CTP heavily promotes the use of the standard form.<sup>83</sup>

In sum, we know that Prevent practitioners can store other personal data, including sensitive personal data, about a person (including a child) who has been referred to the programme. Such information includes:

- Nationality and immigration status;
- Health data, including mental health data;<sup>84</sup>
- Social media accounts;
- Housing status;
- Whether they have been a victim of crime;
- Education and employment status; and
- Information about their families and close networks.

---

<sup>82</sup>Home Office, ['Individuals referred to and supported through the Prevent Programme, April 2023 to March 2024'](#) (5 December 2024); Home Office, ['Individuals referred to and supported through the Prevent Programme, April 2022 to March 2023'](#) (14 December 2023); Home Office, ['Individuals referred to and supported through the Prevent Programme, April 2021 to March 2022'](#) ['Individuals referred to and supported through the Prevent Programme, April 2021 to March 2022'](#) (26 January 2023); Home Office, ['Individuals referred to and supported through the Prevent Programme, England and Wales, April 2020 to March 2021'](#) (18 November 2021); Home Office, ['Individuals referred to and supported through the Prevent Programme, April 2019 to March 2020'](#) (26 November 2020); Home Office, ['Individuals referred to and supported through the Prevent programme, England and Wales, April 2018 to March 2019'](#) (19 December 2019); Home Office, ['Individuals referred to and supported through the Prevent Programme, April 2017 to March 2019'](#) (13 December 2018); Home Office, ['Individuals referred to and supported through the Prevent Programme, April 2016 to March 2017'](#) (27 March 2018); Home Office, ['Individuals referred to and supported through the Prevent Programme, April 2015 to March 2016'](#) (9 November 2017). Home Office data covers only England and Wales; however, police in Scotland appear to record data on similar categories: see Police Scotland, ['Prevent Referral Data'](#) (Police Scotland, updated 2023). Prevent does not apply in Northern Ireland.

<sup>83</sup>See Counter Terrorism Policing Headquarters, ['Policy for Prevent Practitioners: Management of CT/DE Risk within the Community'](#), June 2018, Section Four; Metropolitan Police, 'Freedom of information request reference no: 01.FOI.20.20.015862', no date.

<sup>84</sup>For more information, see Charlotte Heath-Kelly, ['Unhealthy Liaisons: NHS Collaboration with the Counter Terrorism Clinical Consultancy Service'](#) (Medact, 2024).



In recent years, many practitioners have used the template 'Prevent Referral Form' – a document that CTP advises public bodies to use; viewing the form reveals the types of personal information a referring authority might in a Prevent referral (see Annex A). This form was updated in August 2024, with limited changes to the types of data collected, except that in some sections the form now provides specific tick boxes (see Annex B).

Both forms allude to the fact that they entail the collection of certain types of sensitive personal data. However, the 'complex needs', 'relevant behaviours', 'additional factors' and 'safeguarding considerations' sections go further, and request information that might be relevant to a person's 'vulnerability' 'in any sense'. Instead of directing referrers to disclose only information related directly to someone's perceived 'vulnerability' to what the government regards as extremism, the form encourages the sharing of much more extensive personal information, which the government will then store.

Although the government does not publicly highlight the relationship between Prevent and immigration enforcement, the form invites a mention of 'citizenship, asylum or immigration' issues. Similarly, the 'Biographical and contact details' section of the forms include items on 'nationality / citizenship' and 'immigration / asylum status'. The collection of personal data about immigration status sets the stage for the sharing of personal data (including children's data) for immigration purposes, as we discuss further below. Likewise, the post-August 2024 referral form requests data about the referred individual's current and previous employers, schools or universities, risking even further data-sharing about a referral that could have long-term implications for a person's employment or education.

The 'safeguarding considerations' section of the form confirms that Prevent referrals are not consensual. In our report *Secret, Confused and Illegal*, we concluded that '[t]he government often assures practitioners who use Prevent-related personal data that consent is not required – in many instances advising them to avoid seeking consent.'<sup>85</sup>

The model form reinforces this conclusion, asking, 'Have you informed the individual that you are making this referral?'. Arguably, this question could be a nudge toward informing the person. However, it clearly implies that people are not necessarily informed; moreover, informing someone of a referral is not the same as seeking their consent. The form does not state anywhere that consent to a referral is necessary or even desirable.

Similarly, the Government Legal Department (on behalf of the Home Office) told us in correspondence that 'persons referred to Prevent are not generally made aware of their referral unless they are invited to participate in the Channel programme'.<sup>86</sup>

We therefore conclude that Prevent is not a voluntary programme.

---

<sup>85</sup>Rights & Security International, '*Secret, Confused and Illegal: How the UK Handles Personal Data Under Prevent*' (2022), para. 35. Also see the discussion at paras. 11, 31-35, 41-44, 49-50, 57-59, 126 for further information.

<sup>86</sup>Government Legal Department, communication with RSI on behalf of the Home Office, ref no. Z2409530/CB4/DS4, 17 September 2024, para. 5.

## Collection and use of data on racial identity

- Both the police and the Home Office are unable (and, we argue, unwilling) to carry out a fact-based assessment of whether the Prevent referral system is having discriminatory impacts.
- Despite well-known risks of Prevent's disproportionate impact on people who identify as Black, Asian or of Middle Eastern descent (or who are perceived that way), neither the Home Office nor the police are collecting data in a way that would allow them to assess whether Prevent is having a discriminatory impact. The data they collect, as they have admitted to us in correspondence, is too low in quality to make such an assessment possible.
- While the police and the Home Office collect some data on the perceived racial identity of people referred to Prevent, they tell us that they do not do so for statistical or equality monitoring purposes, and they do not do it consistently. In fact, racial identity data (which is based on the perception of the referrer, rather than being self-reported) is only recorded for a relatively small minority of Prevent cases. In the majority of cases, race is not recorded at all, or is recorded as 'unknown'. Figures we have obtained from the government indicate that this trend of missing race data that could have enabled equality monitoring is worsening.
- Instead, the government has told us that it collects racial identity data only sometimes, when it thinks the data could be 'relevant' to the referral. The government has not told us anything further about when and why its Prevent policy-makers think race per se would be relevant to understanding whether someone might engage in violence, or how it avoids what appears to us to be an obvious risk: that Prevent referrers will record an individual's race mainly when the referrers are being influenced by racist stereotypes.

## Collection and use of data on racial identity

- The Home Office and the police told us explicitly that their data regarding the racial identity of people referred to Prevent is likely inaccurate, in part because they do not rely on the individual's description of their own racial identity, instead relying on the referrer's perception.
- The Home Office and the police take a different approach to recording the racial identity of people impacted by Prevent in comparison with their racial impact assessments for other policing and counter-terrorism activities. Both bodies use an '18+1' model – that is, a list of 18 racial/ethnic categories plus an option for 'unknown' – to monitor the impact of other policing and counter-terrorism programmes, but not when they are monitoring the impact of Prevent, when they use only five categories (plus 'unknown'). This inconsistent and broad approach is a factor in the government's inability to discover and monitor any discriminatory impacts of the Prevent strategy.

We are particularly concerned about the collection and storage of data about a person's race or ethnicity (actual or perceived). We note at the outset that 'race' and 'ethnicity' are contested, socially constructed concepts relying on distinctions that are inherently arbitrary, and that the purported distinction between 'race' and 'ethnicity' is arguably artificial. Below, we use the term 'race' to include the concepts of 'ethnicity' and 'national origin', as the legal implications of collecting (or deciding not to collect) data described with any of these labels are similar.

The pre-August 2024 model referral form does not contain a field for Prevent practitioners to note the referred individual's race/ethnicity, but we know (thanks to freedom-of-information requests) that the Home Office and the police have collected and do hold this data for at least some cases. The updated August 2024 referral form does contain a designated 'ethnicity' category.

To determine which public bodies hold Prevent-related data on race, and to gain access to aggregated statistics about the racial impact of Prevent, RSI has submitted several requests under the Freedom of Information Act 2000. After protracted legal processes, the Home Office and the National Police Chiefs' Council (NPCC) – ostensibly acting on behalf of Counter-Terrorism Policing Headquarters (CTP) – have provided us with some of this information; however, this data is incomplete, with race recorded in less than a third of cases.<sup>87</sup> We have included this data at Annexes F, G, N, and O.

The NPCC's, the Home Office's and the Met's responses to our requests indicated generally poor record-keeping and equality-monitoring practices.

As explained further below, the Home Office's and the NPCC's approach to collecting racial impact data related to Prevent is non-systematic, apparently based on guesses or assumptions in at least some instances, and it likely leads to inaccurate reporting and analyses. Despite these serious flaws, we have been able to reach some preliminary conclusions based on the available data, which is limited to people whose cases have been processed by Channel (i.e. not every individual who has been referred to Prevent, since Channel is a later stage of the process). In a previously published analysis, we concluded, *inter alia*:

*'The... data suggests that people recorded as Asian and cases recorded as 'Islamist-related' are subject to comparatively greater scrutiny [under Channel] than other ethnic groups and types of concern.'*

However:

*'People recorded as being from 'White' ethnicities were more likely to be adopted as a Channel case (primarily for right wing related concerns) than people recorded as Asian, although separate Home Office data on terrorism-related criminal sanctions reveal that white ethnicities are less likely to experience the criminal justice outcomes of an arrest, charge or conviction for terrorism-related offences.'*

---

<sup>87</sup>For an overview, see Areeb Ullah, ['UK: Rights groups call on Home Office to investigate 'haphazard' collection of Prevent data'](#) (Middle East Eye, 1 March 2024); Rajeev Syal, ['Police failed to record race of nearly two-thirds of people referred to Prevent'](#) (The Guardian, 6 February 2024).

We inferred from these differences that:

*[A]t a systemic level, officials may view suspected extremism among people from white ethnicities as a concern to pursue through non-criminal sanctions (i.e. Channel), if at all, while viewing suspected extremism among people from Asian ethnicities as a criminal justice matter.’<sup>88</sup>*

While we did not receive all the data we had requested in our freedom-of-information requests, we did obtain some illuminating evidence about the way each of the relevant public bodies (the Home Office, the Metropolitan Police and the NPCC) stores and uses Prevent-related data on race. Some of this evidence concerned the fact that none of these bodies are collecting data about the racial impact of Prevent systematically.

In correspondence with RSI, the Home Office claimed that this dearth of Prevent race data is due to:

a. Prevent referrals being about susceptibility to radicalisation rather than triggered by the presence or absence of a protected characteristic (for example, someone belonging or seeming to belong to a particular race);

b. The fallibility of relying on the referrer’s perception of protected characteristics (that is, people referred to Prevent are not asked to describe their own racial identity, and instead, this is left up to the referrer); and

c. The onerousness of collecting equality data and the resulting risk of dissuading people from making a referral.<sup>89</sup>

We would critique claim (a) on the grounds that it ignores the possibility that a programme will have a discriminatory impact even if it is not discriminatory by design, including because of overt prejudice or unconscious bias on the part of the people implementing it. The phenomenon of discriminatory impact, even without discriminatory intent or design, is well recognised in equality laws globally.

Claim (b) appears to be a self-inflicted problem: both the Home Office and the police have told RSI that their data on the racial impact of Prevent and Channel is likely to be inaccurate because it the PCMT (and other database) entries rely on the referrer’s perception of the individual’s race – that is, the people referred are not asked to describe their own race, including because most never learn of the Prevent referral at all. This practice stands in contrast to other UK policing practices, including counter-terror policing programmes, that rely on asking the people affected to describe their own racial identity.<sup>90</sup> (People asked to provide their racial identity can decline to give this information.)

---

<sup>88</sup>Zin Derfoufi and Sarah St. Vincent, ‘[Analysis of FOI 63470 data on the ethnic composition of Channel cases, and a comparison to the composition of terrorism-related criminal sanctions](#)’ (Rights & Security International, February 2023), p. 2. This analysis is based on data from 2015/16 to 2018/19, as subsequent data was not available at the time.

<sup>89</sup>Government Legal Department, communication with RSI on behalf of the Home Office, ref no. Z2409530/CB4/DS4, 17 September 2024, para. 8.

<sup>90</sup>See, e.g., HM Government, ‘[Criminal Justice System Exchange Data Standards Catalogue – Notification of Change: Introduction of ‘Self Defined Ethnicity – 18+1’ Standard](#)’ (1 March 2018).

## Home Office

When telling us that it does not hold data regarding the race of all – or even most – individuals referred to the Prevent programme, the Home Office claimed that it gathers and stores such data only when the Prevent case officer records an individual's race (or perceived race) as part of the referral process.

The Home Office also confirmed that it does not collect racial data about people impacted by Prevent for statistical purposes – for instance, equality monitoring (that is, tracking whether Prevent disproportionately impacts particular individuals based on protected characteristics such as race, religion or disability). Instead, it claimed that officers only record such data if they believe it is relevant to a specific case. There appear to be no guidelines on when or why a case officer should regard a person's race as relevant and record it, although the Home Office asserted, without further explanation, that race could 'have an impact on an individual's radicalisation'.

The Home Office has also told us that the data it does hold about race is likely inaccurate. The inaccuracy of the Home Office's data is a problem that arises because the racial data stored on the PCMT is based on the case officer's perception of an individual's race, rather than the person's self-defined identity. In our view, collecting race data based on the case officer's perception introduces a clear risk of biases and inaccuracies, undermining the reliability of the data.<sup>91</sup>

Our examination of the practices of other public bodies – including criminal justice agencies and police forces – shows that the Home Office's approach to gathering (or not gathering) data about the racial impact of Prevent is not inevitable and in fact stands outside the norms. For example, many criminal justice data collection practices are premised on the 18+1 or 19+1 category lists of races and ethnicities, which include – for example – an explicit option for people who identify as being from an Arab background.<sup>92</sup> The systemic collection of race data is particularly important for reviewing the potentially discriminatory impact of counter-terrorism practices, and the Home Office itself has used the 18+1 category list when reviewing the operation of police powers under the Terrorism Act 2000.<sup>93</sup> The government has also designated the 18+1 category list for standardised use across the public sector.<sup>94</sup>

By contrast, when collecting the data of people referred to Prevent, the Home Office and the police use a 5+1 category list: 'Asian', 'Black', 'Mixed', 'White', 'Other' and 'Unknown'.<sup>95</sup> These racial identity categories are very broad and could capture many people with different identities within the same category. It may also be difficult for people filling out the Prevent referral form or officers filling in PCMT data entries to gauge where certain identities are best categorised – for example, people identifying as being from an Arab background. Such broad categories make it difficult to gauge and monitor Prevent's actual racial impacts.

---

<sup>91</sup>OHCHR, 'A Human Rights-Based Approach to Data, Leaving No-one Behind in the 2030 Agenda for Sustainable Development' (2018), pp. 11-12.

<sup>92</sup>See Home Office, 'Operation of police powers under the Terrorism Act 2000 and subsequent legislation: Arrests, outcomes, and stop and search, Great Britain, quarterly update to March 2023' (8 June 2023), sections 2.6, 5.1-5.2; Home Office, 'PACE Code A 2023' (20 December 2023), Annex B.

<sup>93</sup>Home Office, 'Operation of police powers under the Terrorism Act 2000 and subsequent legislation: Arrests, outcomes, and stop and search, Great Britain, quarterly update to March 2023' (8 June 2023), sections 2.6, 5.1-5.2.

<sup>94</sup>HM Government, 'Criminal Justice System Exchange Data Standards Catalogue – Notification of Change: Introduction of 'Self Defined Ethnicity – 18+1' Standard' (1 March 2018).

<sup>95</sup>Zin Derfoufi and Sarah St. Vincent, 'Analysis of FOI 63470 data on the ethnic composition of Channel cases, and a comparison to the composition of terrorism-related criminal sanctions' (Rights & Security International, February 2023), p. 5.



It is unclear to us why the Home Office and the police use the 18+1 list to monitor the racial impact of other policing and counter-terrorism powers, but not when they are monitoring the racial impact of Prevent.

Additionally, we know that for other policing and security programmes, the police collect racial identity data based on the individual's self-reported identity, not based on a perception of what that identity might be. For instance, when it comes to the police's use of stop and search powers, officers conducting the searches are obliged to record the self-reported racial identity of the person that they are stopping.<sup>96</sup> The Home Office's annual statistical release on the use of the Schedule 7 Terrorism Act 2000 powers (stop and search as well as detention at ports and airports) also uses the individual's self-defined racial identity rather than their perceived identity.<sup>97</sup> It is unclear why the police and the government takes a different approach to Prevent than it does with other policing and security programmes.

Race data is crucial for the public's and Parliament's ability to understand and assess potential racial disparities in policing, which in turn can point to bias or other problems that the government has a legal responsibility to fix. For example, a recent Home Office data release includes interactive tools to analyse arrests and stop-and-search incidents; these tools allow users to filter data by police force and other variables (such as race) to identify correlations in police activity, while an 'ethnic

disparity time series dashboard' provides graphs to view volumes, search rates, and disparities in police actions regarding minoritised groups compared with people who identify as being from white backgrounds.<sup>98</sup> The Metropolitan Police also provide an online dashboard with race data on stops, searches, and arrests.<sup>99</sup>

By contrast these Home Office's choices regarding Prevent – that is, to collect racial data in some but not all (or even most) instances, and to rely on assessments by the case officer – have resulted in a conclusion by the Home Office itself that the data it holds regarding Channel (the follow-on programme from Prevent) is 'almost certainly not an accurate representation of the ethnicity breakdown of all individuals discussed, adopted and not adopted at Channel.'<sup>100</sup>

It appears as a result that the Home Office is unable to accurately assess whether Prevent relies on bias or whether members of the public sector are using it in a discriminatory way, as Muslim community groups and human rights organisations have long alleged. Given that other data collection practices are clearly available, we are concerned that the Home Office and the police may be choosing not to know what the racial impact of Prevent is, along with the impact on people belonging to certain faiths or who are disabled. Alternatively, the Home Office and the police may be sacrificing the ability to understand the racial, religious and disability impact of Prevent – and thereby disregarding the risk of discrimination – in order to have a secret surveillance programme. More specifically, they would be doing so in order to have a secret surveillance programme focused on children.

---

<sup>96</sup>Home Office, 'Police and Criminal Evidence Act 1984 (PACE) – Code A. Revised Code of Practice for the exercise by: Police Officers of Statutory Powers of stop and search; Police Officers and Police Staff of requirements to record public encounters' (December 2023), paras. 4.3(a), 4.5, 18, 22A. See the list of 'self-defined ethnic classification categories' at Annex B.

<sup>97</sup>Home Office, 'Operation of police powers under TACT 2000, to June 2024' (12 September 2024).

<sup>98</sup>See Home Office, 'Police powers and procedures England and Wales statistics' (Gov.uk, 19 April 2024).

<sup>99</sup>Metropolitan Police, 'Stats and data' (Metropolitan Police, no date).

<sup>100</sup>Quoted from the Home Office's response to RSI's freedom of information request, ref: IC-139957-Z7N2, 14 November 2022 (available at Annex F).

## Policing

The Metropolitan Police and the NPCC – ostensibly on behalf of CTP, which is responsible for managing the main Prevent database<sup>101</sup> – have provided much more limited information to RSI about the way they collect and store Prevent-related data on race. The NPCC has provided us with an explanation that is similar to the Home Office's: they say officers often do not include racial data in the information they collect and store on the PCMT, so any collation of statistics about Prevent and race would reflect incomplete information. However, the NPCC also informed us that '[t]here may be additional ethnicity data contained within the "notes" free text fields' within the PCMT.<sup>102</sup> In June 2024, the NPCC disclosed some data to us concerning the race of people referred to Prevent in England and Wales – statistics we would critique for reasons similar to those set out above regarding Home Office's data. Figures we have obtained from the NPCC indicate that this trend of missing race data that could have enabled equality monitoring is worsening, with the proportion of PCMT records in which no ethnicity is recorded has risen from 38.5 percent in 2018/19 to 57.2 percent in 2023/24.<sup>103</sup> 1. We have since published this data from the NPCC and include it at Annexes N and O.

The Metropolitan Police have described to us a similarly unsystematic approach to the entry and storage of Prevent-related racial data. The Met also told us that it may hold relevant racial data in additional databases such as CRIMINT (apparently a portmanteau of 'criminal intelligence').

Based on the explanation the Met has provided, it appears that the CRIMINT system requires the entry of data about an individual's race; this field cannot be left blank (although it likely includes options such as 'unknown'). However, CRIMINT apparently is not synced with, or cannot aggregate data in a format that can be successfully exported to, the other databases: the Met told RSI that it would 'take over 133 hours' for the agency to review its database entries and collate the recorded racial data of people who have been referred to Prevent. The NPCC has given us an estimate that is even higher: in correspondence with RSI, the body claimed it would need over 1,350 working days to collect the data it needed to assess the racial impact of Prevent.<sup>104</sup> It is unclear why the NPCC and the Met have quoted significantly different figures.

Again, this non-systematic scattering of data across police and Home Office systems points to an inability (or an unwillingness) to assess whether the way these public bodies run Prevent has a disproportionate impact on certain groups in Great Britain, such as people who identify as Black, Asian or of Middle Eastern descent.

---

<sup>101</sup>RSI is still unclear as to why the NPCC rather than CTP are responding to freedom of information requests related to PCMT data.

<sup>102</sup>Further, see, Information Commissioner's Office, [Decision Notice IC-262164-Z2K6](#), 20 December 2023, para. 19.

<sup>103</sup>Rights & Security International, 'New data on Prevent raises racism concerns' (Rights & Security International, 1 October 2024); National Police Chiefs' Council, 'Freedom of Information Request Reference Number: 181/2024' (17 June 2024), p. 2.

<sup>104</sup>Rights & Security International, ['1,350 working days to assess racial impact of Prevent; police data missing, Independent Review silent'](#) (Rights & Security International, 31 January 2024).

## Data input

- The PCMT contains much more data than the public or most UK lawmakers likely realise, including information about 'potential referrals': that is, records of communications about people, including children, who are never actually referred to Prevent.
- The inclusion of 'potential referrals' on the PCMT, a policing database where those records could be maintained for years, misleads teachers, doctors and other Prevent practitioners tasked with engaging with the police about such 'potential referrals'. Meanwhile, the government has incorrectly stated that only formal referrals are recorded on the PCMT.

We have gathered some information about how the PCMT works from official sources, although the available descriptions are limited. From CTP, we have two redacted ‘Quick Reference Guides’ – documents for practitioners on how to use the PCMT – on managing and supervising cases using the system.<sup>105</sup> We also have a redacted Power Point presentation on how to manage cases, which goes into slightly more detail than the guide on the same topic.<sup>106</sup> These documents are indexed on the Metropolitan Police’s website, and were released in response to a series of freedom-of-information requests submitted by another party in 2021.

We have also obtained some information about how the PCMT operates via our own freedom-of-information requests regarding Prevent-related race data.

According to the quick reference guide, there are two options for someone logging a new referral: they can add a new referral to a .....

person’s file if that person (including a child) has been the subject of a Prevent referral previously – as we outlined in Secret, Confused and Illegal, the government can store data relating to Prevent referrals for as long as the police or Home Office deem ‘relevant’<sup>107</sup> – or they can create a new case. If they are creating a new case, then the person entering the personal data can fill in many fields.

The image disclosed on the quick reference guide is unclear in its original form<sup>1</sup>. (see Figure XX); however, we can see that date of birth, age, gender, ethnicity and religion are data fields with ‘drop down’ options.

Unfortunately, the image provided in the disclosed document is of too poor quality for us to assess the other available fields. However, following our own freedom-of-information requests, we know these ‘drop down’ fields are not the only places where police enter personal data into the PCMT.

### Creating a New Subject

If the subject does not exist, the + Create button will be displayed and you can create a new subject.



- Click the + Create a new Individual button.  
**Note:** The New Individual page will be displayed. Complete all of the mandatory information, as well as any additional information you have, for each screen (Individual, Case or Referral). The Case Summary is mandatory and must be completed before progressing.
- Enter all relevant information and click the Save.  
**Note:** all fields marked with a red asterisk \* are mandatory and must be completed before you can save.
- Additional fields become available once each page is saved. To add, click the Click to add link next to the relevant section e.g. email address and once details have been entered, click the Add button.
- Enter all remaining information on each page e.g. case, referral etc. and click the Save button. A new Individual with an associated case and referral has now been created and automatically assigned to the user who created it (Practitioners or Supervisor) as Registered. For any other role permitted to create Subjects, the case owner will be Unallocated.

Figure 3: ‘Creating a New Subject’ PCMT screen

<sup>105</sup>Document Number NCTPHQ/ICT/212 QRG, 24 May 2018 (available at Annex C) and Document Number NCTPHQ/ICT/218 QRG, 30 May 2018 (available at Annex E) respectively.

<sup>106</sup>Document Number NCTPHQ/ICT/215, 31 May 2018 (available at Annex D).

<sup>107</sup>Rights & Security International, ‘Secret, Confused and Illegal: How the UK Handles Personal Data Under Prevent’ (2022), paras. 130-136, 154-155.

Once a case has been opened, authorised Counter-Terrorism Case Officers (CTCOs) and CTCO supervisors can continue to add 'notes' to a file – for instance, when they have visited the referred individual or discussed the case with another professional. We know from our freedom-of-information requests, as described above, that these free text fields may contain sensitive personal information. However, this approach does not seem to support CTP's claim, as part of its training on the PCMT, that the database aids '[i]mproved data accuracy' through the use of 'pre-populated fields and validation'.

The PCMT is also more expansive than might be expected: it includes information about 'potential referrals', which could include thousands of cases in which a referrer is merely expressing a concern rather than actually making referral.<sup>108</sup>

The inclusion of 'potential referrals' on the PCMT also misleads people who wish to raise certain concerns with the police without making an actual Prevent referral; when engaging in these conversations, the person (such as a family member, friend or teacher) may not consent to or even envision the information-sharing that subsequently occurs, but the data they provide will still be stored on the PCMT.

The inclusion of 'potential referrals' on the PCMT also misleads people who wish to raise certain concerns with the police without making an actual Prevent referral; when engaging in these

conversations, the person (such as a family member, friend or teacher) may not consent to or even envision the information-sharing that subsequently occurs, but the data they provide will still be stored on the PCMT. The inclusion of 'potential referrals' on the PCMT appears to contradict government statements that '[only] Prevent referrals that may be appropriate for Channel are recorded on the Prevent Case Management Tracker'.<sup>109</sup>

We are also concerned that the police may have broadened the PCMT's remit so as to create a form of surveillance against particular groups or communities. On slide 7 of Counter Terrorism Policing's PCMT training, the CTP explains that the 'subject' of a database entry can be an '[i]ndividual, [i]nstitution or [i]deology'.<sup>110</sup> While the PCMT is ostensibly a piece of case management software that the police should use solely for individual cases, it appears that the system also includes information about particular groups or – potentially – communities. This information is searchable and sharable.

---

<sup>108</sup>Metropolitan Police, 'Freedom of information request reference no: 01.FOI.20.20.015862', no date; Counter Terrorism Policing Headquarters, 'The Counter-Terrorism Case Officer Guide' (7 December 2020), p. 30.

<sup>109</sup>Home Office, 'Individuals referred to and supported through the Prevent Programme, April 2021 to March 2022' (26 January 2023), section 1.3. See further Home Office, 'Individuals referred to and supported through the Prevent Programme, April 2023 to March 2024' (5 December 2024), section 1.3.

<sup>110</sup>Document Number NCTPHQ/ICT/215, 31 May 2018 (available at Annex D).

## **Prevent as intelligence: The role of FIMUs**

- The PCMT process is secretly run by police intelligence teams within local police forces. Fixed Intelligence Management Units (FIMUs) have a central but poorly understood role throughout the Prevent decision-making process.
- FIMUs are also tasked with 'disrupting' people referred to Prevent. They are also tasked with 'undermining' the 'status/credibility' of people referred to Prevent and 'limit[ing] their activity'. It is unclear what each of these terms mean in this context, but any attempt to interfere with people's – especially children's – lives based on what those people might think, especially when there is no indication that they plan to engage in violence, would raise human rights concerns. Secret surveillance or covert operations, such as a covert effort to embarrass or humiliate someone, would have even greater implications for human rights.
- The centrality of FIMUs in Prevent decision-making shows Prevent for what it really is: an intelligence programme, and one directed mainly at children and teenagers



Many different people have access to data stored in the PCMT. People with direct access include '[a]ny rank of Police Officer or Police Staff...', while '[d]ata entry can be conducted by any Prevent Practitioners [sic] that is authorised to use the database.'<sup>111</sup> CTP has 'immediate access to national subjects and cases' as part of its oversight role.<sup>112</sup> Other public bodies and private intervention providers -- charities that provide in-community support, for example -- also have access to PCMT data when they provide 'support' to somebody who has been referred to Prevent, although their access is not directly through the PCMT.<sup>113</sup>

We also know from the quick reference guides and other sources that Prevent-related personal data is shared with Fixed Intelligence Management Units, or FIMUs, within individual forces.<sup>114</sup> A FIMU's role includes being the focal point of the referral process and directing the case management operators, using Prevent referrals as a form of 'intelligence'. The FIMUs operate secretly, and limited information about them is available, beyond what is listed as part of job adverts and a small quantity of publicly available policy documents.<sup>115</sup>

Although not enough information is available to describe the FIMUs with certainty, it appears that a FIMU's role differs in different regions. For instance, according to the Metropolitan Police, the FIMU does not have direct access to the PCMT, but is frequently informed about the progress of a case and 'must' be informed when a case is closed. In Suffolk, however, the FIMU appears to be granted a greater role: according to the standard operating procedures, 'PREVENT create and submit Police Information Report (PIR) for attention of Special Branch Fixed Intelligence Management Unit (SB FIMU) for assessment', and the FIMU then decides whether the case is suitable for Channel. The Suffolk arrangement seems more likely to be representative of the national picture when it comes to the role of FIMUs in the Prevent process. The Chief Constable of Thames Valley police has written in a letter:

*'[T]he national Prevent process require[s] compliance with the National Standards of Intelligence Management (NSIM)<sup>117</sup> which requires submission of intelligence back into FIMUs as part of the intelligence cycle.'<sup>118</sup>*

<sup>111</sup>South Yorkshire Police, 'Response to Freedom of Information Request – Reference No: 20191213', 18 June 2019.

<sup>112</sup>Document Number NCTPHQ/ICT/215, 31 May 2018 (available at Annex D).

<sup>113</sup>See, e.g. Nottinghamshire Police, '[Nottinghamshire Police Crime prevention](#)' (June 2020), p. 48.

<sup>114</sup>This function was expanded following a recommendation by Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services, as it 'would be useful during initial assessments of Prevent referrals. It would also make sure case updates recorded on the PCMT are available for later assessments.': see Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services, '[Counter-terrorism policing: An inspection of the police's contribution to the government's Prevent programme](#)' (2020), p. 12.

<sup>115</sup>Counter Terrorism Policing, '[Secure Systems Administrator – Fixed Intelligence Management Unit – Police Staff – Counter Terrorism Policing NW](#)' (Counter Terrorism Policing, no date); British Transport Police, '[Fixed Intelligence Management Unit \(FIMU\) Officer](#)' (British Transport Police, no date); Document Number NCTPHQ/ICT/218 QRG, 30 May 2018; Metropolitan Police, 'Freedom of information request reference no: 01.FOI.20.20.015862', no date; Jason Hogg, '[Preventing Future Deaths response of the Chief Constable of Thames Valley Police](#)', letter to The Rt Hon Sir Adrian Fulford PC KC, 15 July 2024; Suffolk Multi Agency Safeguarding Hub, '[Standard Operating Procedures](#)', v6, July 2022; Lancashire Constabulary, '[CTPNW 003-24 Intelligence Management Unit – Detective Sergeant](#)' (Tal.net, October 2024); Bedfordshire Police, '[ERSOU – Counter Terrorism – Prevent Sergeant / Staff Supervisor \(PO1\) – 11286](#)' (Tal.net, November 2022).

<sup>116</sup>Suffolk Multi Agency Safeguarding Hub, '[Standard Operating Procedures](#)', v6, July 2022, p. 30.

<sup>117</sup>This guidance is not publicly available.

<sup>118</sup>Jason Hogg, '[Preventing Future Deaths response of the Chief Constable of Thames Valley Police](#)', letter to The Rt Hon Sir Adrian Fulford PC KC, 15 July 2024.

It appears that FIMUs play a heavy role in Prevent decision-making, as the CTP guidance states that when police are progressing a Prevent case, '[t]he Rationale field should contain an explanation of the reason for moving status. This can simply be the FIMU result through to a detailed explanation for closure.'<sup>119</sup> In fact, the information we have found indicates that Prevent case management officers within the police are told not to progress a case until the FIMU has made a decision about it.<sup>120</sup>

We see FIMUs' role as further support for the conclusion that the PCMT is part of a broader surveillance framework. However, while referring explicitly to 'the intelligence cycle' – which is suggestive of extensive and covert information-gathering – CTP has redacted any further information on this aspect of its process, and there is no further publicly available documentation about how FIMUs and other policing bodies use the 'intelligence cycle' as part of Prevent.

We do know that FIMUs aim to 'disrupt' people who, according to the police, engage in 'extremist' activity – something FIMUs see as a key part of their obligations under the CONTEST counter-terrorism strategy.<sup>121</sup> It is not clear what the government means by 'disruption' in this context, which raises human rights concerns.

Further, the information we have suggests that FIMUs play a central role in Prevent data .....

management, on the basis that they have the potential to see the 'whole intelligence picture'.<sup>122</sup> (Here, we recall again that Prevent mainly impacts children.) Additionally, counter-terrorism case officers, or CTCOs (the people responsible for managing PCMT cases), also '[c]ontinually feed all relevant intelligence to FIMU, throughout the PCM process.'<sup>123</sup> Evidently, therefore, the police want to use Prevent data as a form of intelligence.

Even further, CTCO role descriptions say these officers have the task of 'undermin[ing]' the 'status/credibility' of someone referred to Prevent and 'limit[ing] their activity', regardless of whether they believe the person may have committed any criminal offence.<sup>124</sup> In doing so, police Prevent practitioners can use a 'full range' of investigative powers, including by gaining access to previously obtained mobile phone location records and phone data downloads, as well as collecting information about the person's 'online footprint'.<sup>125</sup>

Again, when it comes to people referred to Prevent, we are mainly talking about children. It is not clear what steps the government might take to 'undermine' and 'limit' a child – or an adult. We observe that there have been – and remain – many controversies in the UK about serious alleged misconduct or highly unethical behaviour by undercover officers, including those spying on activist movements, and this history reinforces our concerns about what it might mean for police or intelligence agencies to try to 'undermine' someone in the Prevent context.

---

<sup>119</sup>Document Number NCTPHQ/ICT/218 QRG, 30 May 2018 (available at Annex E). See also Counter Terrorism Policing Headquarters, 'The Counter-Terrorism Case Officer Guide' (7 December 2020).

<sup>120</sup>Counter Terrorism Policing Headquarters, 'The Counter-Terrorism Case Officer Guide' (7 December 2020), p.30. See also, Bedfordshire Police, 'ERSOU – Counter Terrorism – Prevent Sergeant / Staff Supervisor (PO1) – 11286' (Tal.net, November 2022), 'Role Profile', p. 1.

<sup>121</sup>See, e.g. Lancashire Constabulary, 'CTPNW 003-24 Intelligence Management Unit – Detective Sergeant' (Tal.net, October 2024).

<sup>122</sup>Counter Terrorism Policing Headquarters, 'The Counter-Terrorism Case Officer Guide' (7 December 2020), p. 81. See, e.g. British Transport Police, 'Fixed Intelligence Management Unit (FIMU) Officer' (Tal.net, no date).

<sup>123</sup>Metropolitan Police, 'Prevent/Channel data management: Freedom of information request reference no: 01.FOI.23.029461' (Metropolitan Police, June 2023).

<sup>124</sup>See, e.g. Bedfordshire Police, 'ERSOU – Counter Terrorism – Prevent Sergeant / Staff Supervisor (PO1) – 11286' (Tal.net, November 2022). For further information, see Open Rights Group, 'Prevent and the Pre-Crime State: How Unaccountable Data Sharing is Harming a Generation' (2024), p. 23.

<sup>125</sup>Counter Terrorism Policing Headquarters, 'The Counter-Terrorism Case Officer Guide' (7 December 2020), pp. 81-82.

The referral process and the police's assessment of the referral create the first branches of the spider's web of Prevent data, sending out information to police intelligence units that have the final say on what happens to a referral. This data sharing is only the start of the spider's web of Prevent data. It is possible to gain sight of the other branches by looking at how the police progress a referral.

---

## **Progressing a referral to a Channel panel**

- When the police progress a case to a Channel panel, this decision gives a wide range of public and private bodies access to that individual's personal data; these bodies can then store that data on their own internal databases. For example, local police forces, hospitals and other healthcare providers, or schools.

The Channel Management Information System (CMIS) is the now-redundant database that was run by the Home Office, through which it monitored and managed Channel case records. These records included much of the same information that was included in the old PCMT, but with fewer overall records (since not all people who are subject to a Prevent referral engage with the Channel process; in fact, only a small proportion do).<sup>126</sup> Despite the Home Office's move towards the 'new' PCMT, effectively scrapping the CMIS, the Channel process acts as one of two starting points for the spread of Prevent data – the other being the PCMT itself (see above).

The Home Office's privacy information notice about the Channel process discusses data retention processes:

*'Where information is independently controlled by the Home Office, your data will be stored by the Home Office for 6 years from the date your case is no longer on the programme. Following the closure of your case, all Channel cases are reviewed at 6 months and 12 months. You are no longer on the programme once the 12 month review is complete. Your data will be deleted by the Home Office 6 years from the date of the 12 month review.'*<sup>127</sup>

As Channel is a multi-agency process, many public bodies will sit on a Channel panel, and therefore will have access to personal information included on the PCMT and other police systems.

The Home Office justifies Channel-related information-sharing under s36 of the Counter-Terrorism and Security Act 2015, which gives the Channel process a statutory basis.<sup>128</sup> While the Home Office managed the CMIS (and manages Channel data on the new PCMT), it does not manage individual Channel cases, and therefore much of the Channel data-sharing comes from local police forces or local authorities, depending on the region of the country.<sup>129</sup>

For instance, in August 2021 Lincolnshire Police concluded a Channel-specific information-sharing agreement with several public bodies listed as 'partners' that would gain access to the information: East Midlands Ambulance Service NHS Trust, Lincolnshire County Council, Lincolnshire Partnership NHS Foundation Trust, Lincolnshire Police, NHS Lincolnshire Clinical Commissioning Group, the National Probation Service and United Lincolnshire Hospitals NHS Trust. It also authorises the sharing of Prevent-related data with We Are With You, a charity that offers counselling services.<sup>130</sup> The document does not explain why ambulance personnel or hospitals would need to know about a Prevent referral – or 'potential' referral. (We recall here that someone can make a Prevent referral without having any factual reason to believe that the person in question is violent, and that a large proportion of referrals concern schoolchildren.) The document does not explain why ambulance personnel or hospitals would need to know about a Prevent referral – or 'potential' referral. (We recall here that someone can make a Prevent referral without having any factual reason to believe that the person in question is violent, and that a large proportion of referrals concern schoolchildren.)

---

<sup>126</sup>See South Yorkshire Police, 'Freedom of Information Request – Reference No:20191213' (18 June 2019). The percentage of referrals that led to Channel intervention was approximately 13 percent in the year ending 31 March 2024: Home Office, 'Individuals referred to and supported through the Prevent Programme, April 2023 to March 2024' (5 December 2024), Figure 2.

<sup>127</sup>Home Office, 'Channel data privacy information notice' (Gov.uk, 1 August 2024).

<sup>128</sup>Home Office, 'Channel data privacy information notice' (Gov.uk, 1 August 2024).

<sup>129</sup>Home Office, 'Channel data privacy information notice' (Gov.uk, 1 August 2024).

<sup>130</sup>Lincolnshire Police, 'Channel Programme: Information Sharing Agreement', LP001/F (3 August 2021), pp. 4-5.

It is also possible that Lincolnshire Police or other 'partners' to this agreement have shared personal data with other public or private entities not listed in the agreement.<sup>131</sup>

At least in the Lincolnshire Police example, the partner organisations do not have direct access to the PCMT or other police databases; instead, they receive any information they have requested via 'secure' email. (In this information sharing agreement, Lincolnshire Police do not explain what they mean by 'secure' email – although we infer that they may mean the Criminal Justice Secure Mail (CJSM), which is the secure email platform used by people working in or adjacent to the criminal justice sector, including private companies and charities.)<sup>132</sup> The document says this information is then stored separately on that organisation's internal systems and in line with that organisation's legal obligations and internal policies – meaning that, even when the Lincolnshire Police delete the data they hold, these other bodies may still have access to it.<sup>133</sup>

Reviewing where data goes as part of Channel starts to show the extension of the 'spider's web'. Each of these bodies with Channel data access will have different data protection practices and may further share this data elsewhere. Even if data is deleted from the PCMT, it will likely remain in various policing and non-policing databases – potentially for a long time.

---

<sup>131</sup>Lincolnshire Police, '[Channel Programme: Information Sharing Agreement](#)', LP001/F (3 August 2021), paras. 5.22-5.23.

<sup>132</sup>Lincolnshire Police, '[Channel Programme: Information Sharing Agreement](#)', LP001/F (3 August 2021), paras. 9.1-9.6. On CJSM, see CJSM, '[Welcome to CJSM](#)' (CJSM, no date).

<sup>133</sup>Lincolnshire Police, '[Channel Programme: Information Sharing Agreement](#)', LP001/F (3 August 2021), paras. 10.1-10.2.

## **Secret pathways: Transition to 'Police-Led Partnerships'**

- When the police do not want to seek an individual's consent to the Channel process, or if the person has refused to consent, then the police instead may effectively continue with the Channel process without telling the person involved. Instead, the police will create what the government calls a Police-Led Partnership (PLP).
- As with Channel, when the police create a PLP, this decision allows a wide range of public and private bodies to get access to sensitive personal data about the individual, without the person knowing. The entities that could gain access to the person's data include, for example, the National Crime Agency.
- There is an additional risk that the police will send PLP data to foreign law enforcement agencies, through the involvement of the National Crime Agency. This means, for example, that the police could send data about a child from Iran to the Iranian police.



A Channel intervention is not the only possible outcome of a Prevent referral. In many cases, referrals are diverted to an alternative system – one that does not claim to be a safeguarding scheme at all, but rather strictly a policing one.

Police-Led Partnerships (PLPs) serve as an alternative means of intervention in cases where the FIMU's assessed risk level makes the Channel route unsuitable, in the FIMU's view (in essence, because officers decide the person's risk level is too high for a Channel intervention). However, the police can instead instigate a PLP if the person does not consent to participate in the Channel process, or officers do not want to ask – or even when the Channel panel concludes that its intervention is unnecessary.<sup>134</sup> CTP guidance states that:

*'where a Channel Panel rejects a case as unsuitable, the CTCO must consider whether the issue that brought case into Prevent still remains... Bearing in mind that Police hold, and have final say over, CT risk... If so, then it must be dealt with as a PLP case.'*<sup>135</sup>

CTP thus sees itself as the ultimate arbiter of whether someone is a 'terrorism' risk, regardless of what anyone else involved in the Prevent process concludes – even a Channel panel, which would include other police officers.<sup>136</sup>

As a result, CTP may decide to ignore Channel recommendations and transform a case into a PLP. In this way, the body also has the power to ignore the affected person's decision not to consent to the Channel process. The same CTP guidance states that the PLP panel should have the same composition that a Channel panel would have had, if the person had consented to a Channel intervention.<sup>137</sup> Therefore, if the person does not consent to Channel, they effectively get sent to Channel anyway – in fact, a more secretive version of it. Even if a Channel case ends, a PLP may endure as a form of 'monitoring'.<sup>138</sup>

Police – as per the name – lead PLPs, but they cooperate with other agencies and, in many ways, operate in a similar way to the multi-agency Channel process.<sup>139</sup> For instance, the CTP have concluded data-sharing agreements with local authorities enabling them to share data with one another for the purpose of creating PLP 'support' plans; additionally, if the police later decide that PLP intervention is no longer needed, they can refer the person to other services.<sup>140</sup> Official guidance indicates that all records pertaining to these panels should be retained solely on the PCMT, implying that, in line with PCMT standards, data is stored for at least six years.<sup>141</sup>

<sup>134</sup>See HM Government, 'Prevent duty guidance: Guidance for specified authorities in England and Wales' (2023), pp. 15, 29-30.

<sup>135</sup>CTP, 'CTP-Prevent Policy 2020 Prevent Case Management by CTCOs & CTCO Supervisors' (6 November 2021), p. 28.

<sup>136</sup>CTP, 'CTP-Prevent Policy 2020 Prevent Case Management by CTCOs & CTCO Supervisors' (6 November 2021), p. 28.

<sup>137</sup>In fact, a Channel case and a PLP case may co-exist. In practice, this means that the PLP case is often heard straight after the Channel one, just without the subject's knowledge. See Counter Terrorism Policing Headquarters, 'The Counter-Terrorism Case Officer Guide' (7 December 2020), pp. 63-69.

<sup>138</sup>See Counter Terrorism Policing Headquarters, 'The Counter-Terrorism Case Officer Guide' (7 December 2020), pp. 65-69.

<sup>139</sup>HM Government, 'Prevent duty guidance: Guidance for specified authorities in England and Wales' (2023), p. 15; HM Government, 'Channel duty guidance: Protecting people susceptible to radicalisation: Guidance for Channel panel members' (2023), p. 39.

<sup>140</sup>See CTP-CA-132 Counter Terrorism Policing, 'Purpose Specific Data Sharing Agreement (DSA) Between SO15 Local Operations And Lewisham Local Authority' (22 September 2020), p. 9; CTP, 'Policy for Prevent Practitioners, Management of CT/DE Risk within the Community' (June 2018), p. 18 respectively.

<sup>141</sup>Counter-Terrorism Policing, 'CTP-Prevent Policy 2020 Prevent Case Management by CTCOs & CTCO Supervisors' (6 November 2021), p. 32; Counter Terrorism Policing Headquarters, 'The Counter-Terrorism Case Officer Guide' (7 December 2020), pp. 81-82, p. 64-65.

In the course of their operations, PLPs work with a wide range of partner agencies, such as 'Social Services, the UK Border Agency, the Environment Agency, DVLA [Driving and Vehicle Licensing Agency], Trading Standards, HMRC [the tax authority], and Fundraising Standards Commission'.<sup>142</sup> The PLP selects these partners and decides on their level of involvement in a case based on what they think is relevant to the case.<sup>143</sup> When the decision-making process involves non-policing agencies, the PLP will often make decisions after consulting with these other agencies.<sup>144</sup> As participants in PLP panels, the other agencies have some access to the referred individual's personal data (including the data of a child).<sup>145</sup> The CTP's stated rationale for such extensive data-sharing is that it contributes to the mitigation of Prevent-related risks.<sup>146</sup> However, it does not clarify what kinds of actions social services, the UK Border Agency or the DVLA – for example – might take in the name of lowering these perceived risks (which, as noted above, may be based solely on a hunch and need not be based on any evidence).

In one data-sharing agreement concluded between SO15 Local Operations – the specialist CTP unit tasked with implementing the CONTEST counter-terrorism strategy<sup>147</sup> – and Lewisham Local Authority in 2020, we can see that the agreement allows the police to disclose a broad range of personal data with Lewisham Local Authority, such as information the police have obtained about a person's physical and emotional well-being and parenting (it is unclear whether 'parenting' refers to the individual's parenting style, or their parents', or both), as well as their relatives, family relationships, accommodation and employment status.<sup>148</sup> The agreement also authorises the sharing of data about someone's race, political opinions, religious or philosophical beliefs, and sex life or sexual orientation – all categories of personal data that are supposed to receive especially strong protections under data privacy and human rights laws.<sup>149</sup>

Although CTP guidance indicates that all records pertaining to these panels should be retained solely on the PCMT, several local councils have confirmed in publicly available documents that PLP data is accessible outside of the PCMT.

<sup>142</sup>Counter-Terrorism Policing, '[CTP-Prevent Policy 2020 Prevent Case Management by CTCOs & CTCO Supervisors](#)' (6 November 2021), p. 31.

<sup>143</sup>Counter-Terrorism Policing, '[CTP-Prevent Policy 2020 Prevent Case Management by CTCOs & CTCO Supervisors](#)' (6 November 2021), p. 31.

<sup>144</sup>HM Government, '[Channel duty guidance: Protecting people susceptible to radicalisation: Guidance for Channel panel members](#)' (2023), p. 39.

<sup>145</sup>Counter-Terrorism Policing, '[CTP-Prevent Policy 2020 Prevent Case Management by CTCOs & CTCO Supervisors](#)' (6 November 2021), p. 32; Counter Terrorism Policing, '[Purpose Specific Data Sharing Agreement \(DSA\) Between SO15 Local Operations And Lewisham Local Authority](#)', CTP-CA-132 (22 September 2020), p. 8.

<sup>146</sup>Counter Terrorism Policing, '[Purpose Specific Data Sharing Agreement \(DSA\) Between SO15 Local Operations And Lewisham Local Authority](#)', CTP-CA-132 (22 September 2020), p. 4.

<sup>147</sup>Assistant Commissioner Specialist Operations on behalf of the Commissioner, '[Counter Terrorism Command \(SO15\) review](#)', (12 July 2007).

<sup>148</sup>Counter Terrorism Policing, '[Purpose Specific Data Sharing Agreement \(DSA\) Between SO15 Local Operations And Lewisham Local Authority](#)', CTP-CA-132 (22 September 2020), p. 6.

<sup>149</sup>Counter Terrorism Policing, '[Purpose Specific Data Sharing Agreement \(DSA\) Between SO15 Local Operations And Lewisham Local Authority](#)', CTP-CA-132 (22 September 2020), p. 7. On the additional protection, see [Data Protection Act 2018](#), ss10-11; [Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data](#), ETS No. 108, 1981, Article 6. For a summary of the European Convention on Human Rights' protection for what it describes as 'sensitive data', see European Court of Human Rights, '[Guide to the Case-Law of the European Court of Human Rights: Data protection](#)' (31 August 2022), pp. 11-15.

For instance, Bath and Somerset Council have indicated that PLP board minutes and related documents are stored on a Microsoft SharePoint site, and Coventry City Council echoed this response.<sup>150</sup> The above-mentioned data-sharing agreement between SO15 Local Operations and Lewisham Local Authority from 2020 also indicated that '[i]nformation received from a partner agency will be recorded on PCMT but that if information received constitutes intelligence or a criminal offence, information will also be recorded on CRIMINT or CRIS [(Crime Reporting Information System)]'.<sup>151</sup>

We also know that the UK may send Prevent data to foreign governments as a result of PLPs. This sharing of data with other governments is possible because the National Crime Agency (NCA) has access to Prevent data through being a partner agency for PLP panels; in that role, the NCA can gain access to data about the referred person, including a child or their parents.<sup>152</sup> With official guidance indicating that police should retain all records pertaining to these panels on the PCMT,<sup>153</sup> this may indicate that the NCA has access to the PCMT itself, or at least access to PCMT data through a PLP. Such levels of access to Prevent data are particularly concerning given that the NCA is authorised to share data with foreign governments -- and holds close working relationships with other governments and police forces in a role that it describes as 'supporting diplomacy' (i.e. supporting the UK government's foreign policy objectives).<sup>154</sup>

However, we do not know the range of circumstances in which the NCA might share personal data with its international partners.<sup>155</sup>

It appears that there would be nothing to stop the NCA from sharing highly sensitive personal information about someone in the UK with an abusive government -- even if the person or their family has been persecuted by that other government (for example, because of their political or religious beliefs, or because someone is LGBTQ+).

---

<sup>150</sup>Bath & North East Somerset Council, '[Bath & North East Somerset Council Request for Information](#)' (24 May 2023) p. 3; Coventry City Council, '[Freedom of information request reference no: FOI500145498](#)' (24 April 2023) p. 3.

<sup>151</sup>CRIS is the Crime Reporting Information System, which we do not discuss in this report. Counter Terrorism Policing, '[Purpose Specific Data Sharing Agreement \(DSA\) Between SO15 Local Operations And Lewisham Local Authority](#)', CTP-CA-132 (22 September 2020), p. 15.

<sup>152</sup>CTP, '[CTP-Prevent Policy 2020 Prevent Case Management by CTCOs & CTCO Supervisors](#)' (6 November 2021), p. 32; CTP-CA-132 Counter Terrorism Policing, '[Purpose Specific Data Sharing Agreement \(DSA\) Between SO15 Local Operations And Lewisham Local Authority](#)' (22 September 2020), p.9.

<sup>153</sup>CTP, '[CTP-Prevent Policy 2020 Prevent Case Management by CTCOs & CTCO Supervisors](#)' (6 November 2021), p. 32.

<sup>154</sup>E.g. see National Crime Agency, '[International network](#)' (NCA, no date).

<sup>155</sup>By virtue of the [Crime and Courts Act 2013](#), s7. See National Crime Agency, '[Privacy and Cookie Policy](#)' (National Crime Agency, no date), section 10.

# Prevent as policing: Extending the 'spider's web'

- The police duplicate PCMT records and copy them into other policing databases that are not related to Prevent, including databases for storing criminal offence data and 'intelligence'.
- The police may store Prevent data in these other policing databases for much longer than in the PCMT. If someone refers a child to Prevent when the child is 15, the child's personal data will remain in the Police National Computer (PNC) for another 85 years, while at least in theory, their data would only appear in the PCMT until they turned 21 (assuming that the government did not extend the retention period).
- The storage of Prevent data on other policing databases rapidly expands the range of people and public bodies that have access to this data. Entities with access to such data include MI5, MI6, His Majesty's Revenue and Customs (the UK tax authority) and the Charity Commission, which regulates nonprofits.
- The Home Office also has access to Prevent data contained within these policing databases, and it searches these databases when making decisions about somebody's application for naturalisation as a British citizen. A Prevent referral could therefore impact someone's citizenship.
- Local police forces have access to these non-Prevent-related policing databases, and many of them (either automatically or manually) sync records with their national equivalents. Therefore, data about a Prevent referral could end up all over the country.
- As a result of this extensive duplication and sharing, Prevent data also ends up in other secretive databases, for example those run by the Ports Authority and the UK Border Force. Such practices lead to significant 'mission creep' and show the even broader potential impact a Prevent referral can have.

The use of PLPs to avoid the Channel process is only the start of the extensive policing and, in reality, surveillance that can result from a Prevent referral. Outside of policing bodies, CTP guidance also states that data-sharing among police forces and with 'local authority partners' is 'permitted, and in some cases required, through existing legislation'.<sup>156</sup> It is this extensive sharing and duplication of Prevent data that causes the spider's web of Prevent data to become massive.

## Police National Computer

**Police National  
Computer (PNC)**

**Managing bodies:**

**Home  
Office**



---

**Bodies with access to data:**

**Home  
Office**



**Border Force**



---

**Years  
data is  
held:**

**100**

Until the  
individual's  
100th  
birthday

Police officers will use information obtained for the purposes of a Prevent referral and copy it into other systems and databases – often ones the police use solely for policing purposes.<sup>157</sup> The main policing database is the Police National Computer (PNC).

The PNC is a national database that the police primarily use for their day-to-day work, and it has many in-built functions; however, its main role is to show 'details of convictions, cautions, reprimands, warnings and arrests'.<sup>158</sup> At the same time, the PNC contains a wealth of personal data and other information, and it allows officers to search ANPR (automatic number plate recognition) and VDOS (vehicle descriptive online search) systems for vehicles, enabling location tracking; CRIMELINK for previously reported crimes and suspected crimes; and QUEST (Querying Using Enhanced Search Techniques) for individuals based on descriptions of their personal features.<sup>159</sup> Not all officers have full access to the database: individual forces make decisions about which officers should have access to which data.

The Home Office has said it is planning to replace the PNC with what it calls the Law Enforcement Data Service (LEDS), as the software underlying the PNC will no longer be supported from the end of 2024. (At the time of writing, the Home Office's plans have been delayed, and it appears that the authorities will be migrating to a modified version of the PNC for at least a year while the development of LEDS continues.)<sup>160</sup>

<sup>156</sup>Counter Terrorism Policing, '[CTP-Prevent Policy 2020 Prevent Case Management by CTCOs & CTCO Supervisors](#)' (6 November 2021), p. 32.

<sup>157</sup>Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services, '[Counter-terrorism policing: An inspection of the police's contribution to the government's Prevent programme](#)' (2020), p. 12. The police and Home Office also allude to this data sharing in their responses to our freedom of information requests, outlined elsewhere in this report.

<sup>158</sup>The PNC was created in pursuance of the [Police and Criminal Evidence Act 1984](#), s27(4). Quote from Jacqueline Beard and Lulu Mead, '[Criminal records](#)' (House of Commons Library, 13 July 2023).

<sup>159</sup>[Police National Computer](#), in Graham Gooch and Michael Williams (eds.), *A Dictionary of Law Enforcement* (Oxford: Oxford University Press, 2014).

<sup>160</sup>Eliot Beer, '[Police National Computer replacement runs risk of further 3-year delay](#)' (The Stack, 2 March 2022).

The Home Office is introducing the LEDS on what it calls an ‘incremental’ basis, meaning that both the LEDS and the PNC will co-exist for an unspecified time until the LEDS is fully operational – leading to a duplication of records on each system.<sup>161</sup>

Each of these functions involves the storage or processing of personal data. A person’s (including a child’s) PNC record will generally contain information about their name, date of birth, sex and race/ethnicity (as perceived by the officer reporting the data for entry onto the system). Records can also include DNA profiles and fingerprints, as well as information about any arrests or convictions.<sup>162</sup>

We also know that the PNC contains Prevent-related data – even though the PNC is a database for storing alleged criminal offence data, whereas Prevent is a programme specifically for people who have not committed a crime and are not suspected of planning one. This storage of Prevent data in the PNC raises concerns about how the police and other public bodies use Prevent-related data.

First, this practice creates a problem regarding retention periods. In contrast to the storage of data in the PCMT, which lasts for at least six years, the police retain can records in the PNC until the person reaches their 100th birthday.<sup>163</sup>

Although people can apply to have records removed from the PNC, the police do not delete any personal data proactively.<sup>164</sup>

The sole exception concerns biometric data or DNA data, which the police can store for a range of different time periods. If the person is arrested, the police can store that data for up to two years with the agreement of a district judge or three years if approved by the Biometrics Commissioner; if somebody has committed a ‘qualifying offence’ or an adult has committed a ‘recordable offence’, then the police may hold their biometric data indefinitely.<sup>165</sup> Therefore, if someone refers a child to Prevent when the child is 15, the child’s personal data will remain in the PNC for 85 years (in most cases, the rest of their lives), while at least in theory, their data would only appear in the PCMT until they were 21 (assuming that the government did not extend the retention period, which it has given itself the power to do under current policy).

The storage of Prevent-related data on the PNC rapidly expands the range of people who can access it, as it means that police officers without counter-terrorism or Prevent-specific roles are able to view this information.<sup>166</sup>

This practice also broadens the range of people other than regular police forces who have access to the data, outside the original purpose of the referral. For instance, members of MI5 and MI6 also have full access to the PNC, meaning that a Prevent referral could subject to longer term surveillance and monitoring by the security services. Other non-policing bodies such as the Home Office; the UK Border Agency; and the Foreign, Commonwealth and Development Office also have limited access to PNC data: they cannot

---

<sup>161</sup>College of Policing and Home Office, ‘[Code of Practice for the Police National Computer \(PNC\) and the Law Enforcement Data Service \(LEDS\)](#)’ (23 February 2023), Part 1.

<sup>162</sup>For a summary, see Home Office, ‘[Police National Computer](#)’, v5.0, 23 January 2014, pp. 5-8. See also Jamie Grierson, ‘[What the loss of records from the Police National Computer means](#)’ (The Guardian, 15 January 2021).

<sup>163</sup>There appears to be no publicly available policy document that references this: see Jacqueline Beard and Lulu Mead, ‘[Criminal records](#)’ (House of Commons Library, 13 July 2023).

<sup>164</sup>For an overview, see ACRO Criminal Records Office, ‘[Record Deletion](#)’ (ACRO, no date). For more information, see National Police Chiefs’ Council, ‘[Deletion of records from national police systems \(PNC/NDNAD/IDENT1\)](#)’, version 2.1 (2018).

<sup>165</sup>See National Police Chiefs’ Council, ‘[Guidance: record deletion](#)’, version 2.1 (2023), Annex C.

<sup>166</sup>Child Rights International Network, ‘[Preventing Safeguarding: The Prevent Strategy and children’s rights](#)’ (2022), p. 46.



create or edit entries in the system, but are able to view certain parts of the PNC or certain parts of individual entries.<sup>167</sup> For example, we know that police forces may share PNC data with the Home Office to assist the latter with immigration decisions – and this data could include information relating to a Prevent referral.<sup>168</sup> The Charity Commission – a regulatory body that civil society has accused of being politicised and targeting Muslim-led and Muslim community organisations in the past – also has this level of access to PNC data.<sup>169</sup> Private researchers may also request access to PNC data for statistical analysis.<sup>170</sup>

We also know that the Home Office may conduct searches of the PNC when making decisions relating to someone's application to naturalise as a British citizen. To become a British citizen, applicants must satisfy the Home Office that they are of 'good character' – a requirement under British nationality law that is very broad and not defined.<sup>171</sup> In practice, caseworkers use their discretion to decide whether applicants (including children) are of 'good character' by taking into account factors such as criminal records (including police interactions that did not result in any charges or convictions), prior breaches of immigration law, and financial status (such as debt).<sup>172</sup>

Given the opaque nature of the 'good character' requirement and the assessments decision-makers undertake, an unjustified Prevent referral, which will normally remain on the PNC no matter how baseless it is, could

potentially cause someone's naturalisation application to be refused for failing the 'good character' test. This and other problems with the 'good character' requirement are the subject of a forthcoming RSI report.

The Home Office and other immigration authorities, such as the UK Border Force, also have access to other Prevent databases or policing databases that contain Prevent-related data. We address some of these further below.

We also know from the model referral form (reproduced in Annexes A and B) that referrers are asked to include information about the referred person's immigration and asylum status, as well as their nationality and citizenship. The consideration of information about immigration and asylum status as part of the referral (and subsequent) process leads to real concerns about whether and how Prevent referrals – including those the authorities have already decided require no further action – may impact the immigration or asylum process.

Further, following the conclusion of the Independent Review of Prevent in 2023, the government has explored the possibility of extending the 'Prevent duty' – that is, the legal obligation to report people for ostensibly being at risk of 'being drawn into terrorism', even when there is no evidence to support this suspicion – to Immigration Enforcement and Jobcentre Plus when it comes to their engagement with asylum-seekers and unemployed people seeking help, respectively.<sup>173</sup>

---

<sup>167</sup>Unlock, '[Organisations that have access to the Police National Computer \(PNC\)](#)' (Unlock, no date).

<sup>168</sup>The NPCC states that forces should share both 'basic information' and 'additional information' with the Home Office, which essentially includes all information that might be stored on the NPC: National Police Chief's Council, '[Information sharing with the Home Office where a victim or witness of crime is a suspected immigration offender](#)' (1 April 2022), paras. 6.1-6.2. This information sharing is under the authority of the [Immigration and Asylum Act 1999](#), s20 and the common law.

<sup>169</sup>See, e.g., Randeep Ramesh, '[Quarter of Charity Commission inquiries target Muslim groups](#)' (The Guardian, 16 November 2014).

<sup>170</sup>See e.g. Institute for Fiscal Studies, '[The Police National Computer \(PNC\) data](#)' (IFS, no date). For information on government policy on this point, see HM Government, '[Data sharing guidance for researchers seeking permission for secure access to data](#)' (January 2022).

<sup>171</sup>[British Nationality Act 1981](#), s9; [Nationality and Borders Act 2022](#), Schedule 1.

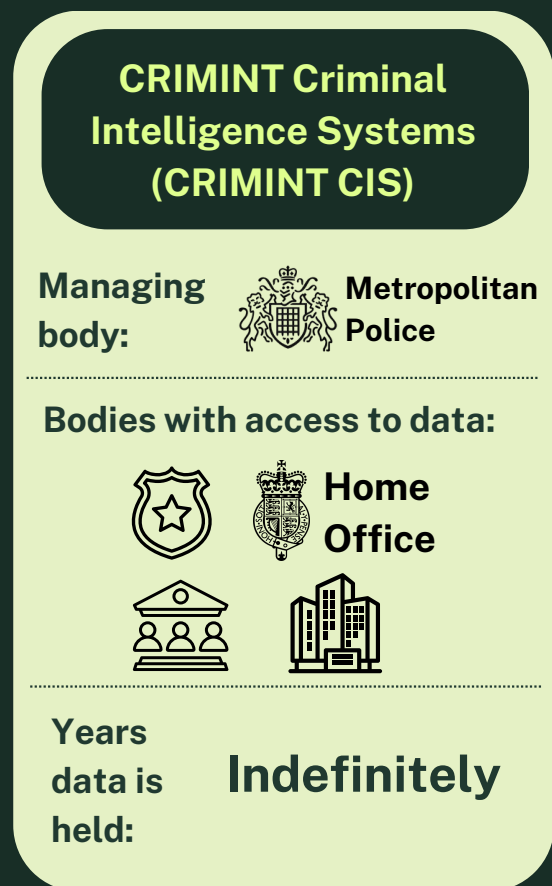
<sup>172</sup>Home Office, '[Nationality: good character requirement](#)' (31 July 2023). See, e.g. [MB v. Secretary of State for the Home Department](#), SN/47/2015, 22 December 2016; [Mustafa Ates \(MUA\) v. Secretary of State for the Home Department](#), SN/96/2021, 17 January 2023.

<sup>173</sup>William Shawcross CVO, '[Independent Review of Prevent](#)', HC 1072, February 2023, paras. 6.5-6.10; Home Office, '[Independent report: The response to the Independent Review of Prevent](#)', 13 December 2023, response to Recommendation 8.

(RSI has previously published evidence suggesting that the Independent Review was not, in fact, independent from the government.)<sup>174</sup> Such a move would likely contribute to the increased storage of immigration- and asylum-related data on Prevent databases – and to a possibility that any interaction with government authorities, at all, could lead to a Prevent referral and ultimately a loss of immigration status.

For anyone familiar with the handling of criminal justice and ‘intelligence’ data today, a question will immediately arise about whether data from the PNC or other large systems, including Prevent data, is subjected to ‘predictive policing’ or other AI analyses – potentially using controversial software marketed by private companies. We do not know the answer to this question, meaning that we do not know if – for example – an AI analysis of Prevent data, potentially along with other police data sources, is resulting in additional surveillance of a person, visa or citizenship application rejections, cancelled immigration status or other serious consequences. We are also not aware of any provision of law or policy that would stop the government from subjecting people – including children or their families – to ‘predictive policing’ in this way if they have been caught up in Prevent.

## Criminal Intelligence (CRIMINT)



The CRIMINT Criminal Intelligence System (CRIMINT CIS) is an example of a criminal intelligence database used by the Metropolitan Police. CRIMINT databases are distinct from the PNC in that they focus on ‘intelligence’ information, not necessarily information linked to alleged crimes. Additionally, each force operates its own CRIMINT system, whereas the PNC is (as the name suggests) a UK-wide system.

In the past, the Metropolitan Police have used the CRIMINT CIS system to track protesters and journalists.<sup>175</sup>

<sup>174</sup>Lizzie Dearden, ‘Home Office accused of ‘interference’ in delayed review of Prevent counterterror scheme’ (The Independent, 23 January 2023).

<sup>175</sup>See e.g. Paul Lewis and Marc Vallée, ‘Revealed: police databank on thousands of protestors’ (The Guardian, 6 March 2009).

Although we do not know if this practice persists today, we do know that the police define 'intelligence' broadly, meaning that over the past decade, human rights groups have raised concerns about the police hoarding data on the CRIMINT system.<sup>176</sup> (We observe here that 'intelligence' simply means information; it is not necessarily correct or relevant to any investigation.) We also know that personal data ends up in the CRIMINT databases when the authorities copy it from other police systems, such as the PNC.<sup>177</sup>

For example, in response to one of RSI's freedom-of-information requests, the Metropolitan Police told us they have access to the racial identity data of people referred to Prevent via the CRIMINT system – indeed, race/ethnicity is a 'mandatory' field in CRIMINT; however, at the same time, they said it would be difficult to collate this information because it is not a pre-defined 'field' or 'box'.<sup>178</sup> It is unclear to us how the collection of ethnicity data can be mandatory, yet not require the completion of a pre-defined field or box.

The upshot is that even though some police forces claim they monitor the equality impacts of their work,<sup>179</sup> they do not collect or store this data in a way in that would allow them to see (let alone evaluate) the racial impact of Prevent. To the best of our knowledge, this inability to carry out a fact-based equality impact assessment is also true for religious identity or belief, as well as disability.

On the CRIMINT CIS database, police may store data about people's interactions with police for a limited period of time, depending on the type of offence allegedly committed; however, police often store 'intelligence' data there for undefined and potentially longer periods.<sup>180</sup>

## Police National Database



<sup>176</sup>See Ryan Gallagher, 'Police share more than 50m records about members of the public' (The Guardian, 21 August 2012).

<sup>177</sup>College of Policing, 'Intelligence collection, development and dissemination' (16 March 2015), 'Tasked information' and 'closed sources'.

<sup>178</sup>FOI reference 01/FOI/23/029393, 18 May 2023 (available at Annex H).

<sup>179</sup>For an overview, see South Wales Police, 'Equality Impact Assessment: A practical tool to eliminate discrimination' (9 May 2023).

<sup>180</sup>See e.g. Metropolitan Police, 'Records Management Policy Toolkit – Management of Police Information (MoPI) Group Table to inform records Review Retention and Disposal (RRD)' (8 July 2015, reviewed January 2019).

CRIMINT data also gets uploaded to the Police National Database (PND). In contrast to the PNC, which is used for criminal offence data, the police use the PND for 'soft' intelligence in cases where investigations did not lead to prosecution.<sup>181</sup> The stated purpose of the PND is to ensure that all police forces have access to the same 'intelligence' information; in that regard, the PND is 'an intelligence data-handling system rather than an evidential system.'<sup>182</sup> The database contains over two billion entries, with twenty million new entries added each month, while merging data from 220 databases controlled by 53 different law enforcement agencies.<sup>183</sup> Although we do not know how many of these 220 databases contain data from Prevent referrals, we know that CRIMINT systems are among the databases synced with the PND, meaning that data that individual forces store in CRIMINT systems will also be uploaded to the national database. We do not know whether data in the PND is subjected to AI analyses, such as 'predictive policing'.

Some forces can upload information to the system automatically;<sup>184</sup> however, forces have discretion as to how to engage with the PND.<sup>185</sup> For example, the Metropolitan Police automatically upload information related to their 'five core business areas' (including CRIMINT information) to the PND each day.<sup>186</sup>

These divergent practices create a foreseeability problem that adds to the existing lack of clarity around where Prevent data is stored, who has access to it, and how it is used.

In practice, these diverging approaches among police forces mean that one person's Prevent data may automatically be copied from the local CRIMINT system to the PND, whereas another's may not be duplicated at all – adding to a person's inability to know where their data is going.

But data-sharing goes even further than simply uploading records to the PND: it also involves the transfer of records from the PND to other local police forces' systems. The Code of Practice on the use of the PND gives local forces the power to take information from the PND and use it for other purposes, including storing it on their own internal databases.<sup>187</sup> Different police forces use the PND in different ways, creating a similar foreseeability issue to that described above.<sup>188</sup>

By policy, PND records are generally deleted after six years unless the police believe the person poses an ongoing risk; we do not know if these decisions are individualised, or whether officers can decide that entire groups or categories of people are still an ongoing risk.<sup>189</sup> We also do not know what criteria, if any, the police use when deciding whether someone – or some group of people – poses an ongoing risk.

---

<sup>181</sup>Jacqueline Beard and Lulu Mead, 'Criminal records' (House of Commons Library, 13 July 2023). As with the PNC, the PND is managed by the Home Office and owned by the National Police Chiefs' Council: see Committee of Public Accounts, 'The National Law Enforcement Data Programme', Twenty-Ninth Report of Session 2021-22, 8 December 2021.

<sup>182</sup>Her Majesty's Inspectorate of Constabulary, 'Building the Picture: An inspection of police information management: The Metropolitan Police Service' (July 2015), p. 11; National Policing Improvement Agency, 'Code of Practice On the Operation and Use of the Police National Database' (March 2010), p. 6.

<sup>183</sup>Datalynx, 'Police National Database' (Datalynx, no date).

<sup>184</sup>Datalynx, the company that assisted all UK police forces in accessing the PND, said that it created the '[a]utomated [s]haring of [i]ntelligence': Datalynx, 'Police National Database' (Datalynx, no date).

<sup>185</sup>National Policing Improvement Agency, 'Code of Practice On the Operation and Use of the Police National Database' (March 2010), p. 6.

<sup>186</sup>Her Majesty's Inspectorate of Constabulary, 'Building the Picture: An inspection of police information management: The Metropolitan Police Service' (July 2015), pp. 9-11. The current CRIMINT CIS was not fully operational during the Metropolitan Police's inspection.

<sup>187</sup>National Policing Improvement Agency, 'Code of Practice On the Operation and Use of the Police National Database' (March 2010), p. 8.

<sup>188</sup>See Rebecca Phythian and Stuart Kirby, 'What does the UK Police National Database tell us about the future of police intelligence?' (2023) 17 Policing: A Journal of Policy and Practice 1-14.

<sup>189</sup>For a summary, see Jacqueline Beard and Lulu Mead, 'Criminal records' (House of Commons Library, 13 July 2023).

Regardless of when (if ever) the police delete PND data, this information may still remain on the local police force's CRIMINT system (CRIMINT CIS for the Metropolitan Police) and the PNC long after it is deleted from the PND: we know these other systems entail significantly longer data retention periods.

This broad sharing and automatic uploading of Prevent data contributes to a complex spider's web of databases, all of which may contain personal data related to a Prevent referral (including the referral of a child). Even when data is removed from one policing system, it may and probably does remain on others.

## Ports Authority Watchlist and the Warnings Index

### Ports Authority Watchlist (PAW)

**Managing bodies:** Unknown

**Bodies with access to data:**



Border Force



COUNTER  
TERRORISM  
POLICING

**Years data is held:**



### Warnings Index (WI)

**Managing bodies:**  Border Force

**Bodies with access to data:**



Border Force



UK Visas and  
Immigration



**Home  
Office**



**Years data is held:**



Unknown

There is a great deal of secrecy around the Ports Authority Watchlist (PAW) database, which is the UK's counter-terrorism database for ports. We are concerned that the PAW might enable the misuse of Prevent data at airports, ports and train stations.<sup>190</sup>

Referred to as the 'Ports Intelligence Watchlist' in the Metropolitan Police's 'Prevent case management guidance', the PAW also has links to the Warnings Index (WI) and Border Force Intelligence (BFI) – two other immigration-related databases.<sup>191</sup> The WI is a database run by the UK Border Force and contains immigration data, data about interactions with police and the criminal justice system, and 'intelligence' that is unrelated to any suspected crime or any policing activity.<sup>192</sup> The UK Border Force says it uses the WI to identify and address criminal, security and immigration concerns.<sup>193</sup> Meanwhile, the BFI is the law enforcement entity within the UK Border Force 'tasked with securing the border and protecting the public against terrorism, crime, revenue fraud, and immigration abuse'. It has four separate regional entities, while the national Border Force National Intelligence Hub (BFNIH) is responsible for allocating the workload among these bodies.<sup>194</sup>

We also know that BFI collaborates with multiple agencies, including the Counter Terrorism Border police, under a Gateway Multi-Agency Hub; while this process has many stated goals, the government says it mainly uses the system to investigate suspected immigration-related crimes and for counter-terrorism purposes.<sup>195</sup> The BFI also uses the PNC as part of its duties.<sup>196</sup>

However, the Home Office has recognised the WI as being 'increasingly expensive, difficult to maintain and unfit for the future needs of government'.<sup>197</sup> As of 2022, the government, as part of plans to replace the WI, had spent £692.8 million developing Digital Services at the Border (DSAB), a 'major programme seeking to deliver the transformational functionality for future improvements needed for the national security and protection of our country, and facilitate improvements to business operations, plus replace legacy technology'.<sup>198</sup> With few or no updates available since late 2022, uncertainty surrounds the potential launch, status, abandonment or further postponement of the DSAB. Should the WI remain active, questions emerge regarding the reasons for its continuation, particularly given the open criticism from the Home Office itself.

<sup>190</sup>Mark Townsend, [Revealed: data from UK anti-radicalisation scheme Prevent being shared with ports and airports](#) (The Guardian, 17 December 2023).

<sup>191</sup>Metropolitan Police Service, ['CTP Prevent Policy 2020'](#), released under 01.FOI.21.021978; Home Office, [The response to the Parliamentary and Health Service Ombudsman investigation into a complaint by Mrs A and her family about the Home Office](#) (January 2015), p. 33.

<sup>192</sup>The Rt Hon Amber Rudd MP, [Inquest into the Death of Alice Poppy Madeline Gross – Regulation 28 Report](#) (6 September 2016), p. 5.

<sup>193</sup>The Rt Hon Amber Rudd MP, [Inquest into the Death of Alice Poppy Madeline Gross – Regulation 28 Report](#) (6 September 2016), p. 5.; Independent Chief Inspector of Borders and Immigration, ['Exporting the border? An inspection of e-Borders'](#), (October 2012-March 2013), p. 50.

<sup>194</sup>Independent Chief Inspector of Borders and Immigration's, [An inspection of the Border Force intelligence functions at the Humber ports](#), (June 2022 – November 2022), p.90; Home Office, [The response to the Parliamentary and Health Service Ombudsman investigation into a complaint by Mrs A and her family about the Home Office](#) (January 2015), pp.24-25.

<sup>195</sup>Independent Chief Inspector of Borders and Immigration, [An inspection of the Border Force intelligence functions at the Humber ports](#), (June 2022 – November 2022), p. 56; Devon and Cornwall Police and the National Police Chief's Council, ['Modern Slavery and Organised Immigration Crime Programme: Annual Report 2021-22'](#) (2022), pp. 21-22; Devon and Cornwall Police and the National Police Chief's Council, ['Modern Slavery and Organised Immigration Crime Programme: Annual Report 2020-21'](#) (2021), p. 38.

<sup>196</sup>Independent Chief Inspector of Borders and Immigration, [An inspection of the Border Force intelligence functions at the Humber ports](#), (June 2022 – November 2022), pp. 181-182.

<sup>197</sup>Home Office, ['Digital Services At the Border, Report by the Comptroller and Auditor General'](#) (7 December 2020), p.5.

<sup>198</sup>Home Office, ['6 September 2022: Digital Services at the Border \(DSAB\) accounting officer assessment'](#) (Accessed: 06 June 2024). See also, House of Lords, ['Written Statements and Written Answers'](#) (5 September 2022), p. 30; Sam Trendall, ['Legacy costs take spending on digital border programme to £700m'](#) (Civil Service World, 11 August 2022).

<sup>199</sup>





With such little information available, we do not know how PAW works, its purpose, or what data the government stores there. This lack of clarity creates reasons to be concerned about the ways the police and other bodies might use the database. Regardless, the potential affiliations of PIW with multiple agencies, combined with the BFI's use of PNC, contribute to a further understanding of the Prevent strategy's reliance on a confusing spider's web of databases accessible to an unknown number of bodies. Similar to other Prevent databases discussed above, such as the CMIS, the PAW is unlikely to meet the accessibility and transparency thresholds demanded by law, leaving individuals with no real avenues for ascertaining whether their personal data is retained, the nature of that information, or where it is held.

# Analysis and Conclusions

Under Article 8 of the European Convention on Human Rights (ECHR), governments are obligated to uphold everyone's right to respect for their private and family life. This duty includes a requirement that laws governing the collection and handling of a person's private information must be clear, accessible, and stipulate the circumstances under which the government or other institutions can process the personal data.<sup>199</sup> By establishing a convoluted spider's web of databases, the UK government has created an environment in which people – such as children and their parents – will have almost no idea where their personal data is stored, what the data includes, whether it is correct, who has access to it and what the consequences could be (if those people are even notified of the Prevent referral in the first place, which usually will not be the case).

In practice, the government's approach means virtually no one can hold it accountable for any illegal sharing or use of personal data under Prevent.

These breaches of Article 8 also have implications for other human rights, such as the freedoms of religion, expression, and association or assembly (Articles 9, 10 and 11), as well as the right to be free from discrimination regarding any of these other rights (Article 14).

Prevent is a programme that impacts thousands of people in Great Britain, most of them children, every year. That means the scale of these harms and potential harms is serious and deserves attention from the UK government at the highest levels.

It is not acceptable under international law to ignore a known problem that harms thousands of children annually, including a large number of children from minoritised groups.

## The collection of race data and the monitoring of equality impacts

The police's broad use of personal information becomes particularly concerning in human rights terms when coupled with our understanding of how the police and other public bodies in Great Britain use data from Prevent, as well as our understanding of how Prevent disproportionately impacts – or could disproportionately impact – certain groups of people.

We have explained that the police and the Home Office collect data about the racial identity of people referred to Prevent, but only unsystematically and unreliably, with the information based on the referrer's perception of the individual's race. There is also a distinct lack of fact-based equality monitoring.

Given broader documented patterns in policing in Great Britain, as well as the specific history of Prevent, we conclude that it is extremely likely that Prevent disproportionately impacts Muslims and members of minority racial groups, along with people with disabilities. Police, the Home Office and government ministers would have every reason to anticipate this problem and carry out data collection and monitoring to forestall it. Yet, those obvious steps are not happening.

---

<sup>199</sup>For further discussion on the UK's obligations under Article 8 in relation to data collection see, Rights & Security International, '[Secret, Confused and Illegal: How the UK Handles Personal Data Under Prevent](#)' (2022), pp. 37-47.

Collecting data about race is crucial for equality monitoring. Regarding violence prevention, however, it is not clear to us when or why the Home Office or police believe race is relevant – such that they collect data about it some of the time, but not all or even most of the time. It is difficult for us to avoid the conclusion that there is no standard Home Office or police policy regarding when race is ‘relevant’ to a Prevent case, and that the most obvious potential reason for someone to include race data in a Prevent referral – especially given the apparent lack of rules – would be racism: that is, people making Prevent referrals are probably more likely to record information about a person’s race when the referral is influenced by racial stereotyping. Insofar as Prevent is intended to capture information about people because of their beliefs or opinions, we note that race is not a proxy for those things.

When collecting race or other data about protected characteristics for equality monitoring purposes, relying on the subject’s self-reporting rather than the case officer’s perception is essential. The spectre of an officer simply guessing whether a person is Black, Asian or ‘Mixed’ – for example – is a disturbing one, and rightly so. Self-reporting minimises inaccuracies and therefore facilitates a more reliable assessment of racial disparities. It is also, in our view, important for human dignity. No one should be subjected to having a police officer, teacher, professor or health care worker try to guess their race.

Regardless of the specific mechanisms various agencies may have adopted for collecting and storing Prevent-related racial data, it is evident

from the responses to our freedom-of-information requests that the Home Office, the NPCC and the Metropolitan Police pay little or no regard to whether the way they operate Prevent has discriminatory impacts on Both the NPCC (initially) and the Metropolitan Police refused to disclose to RSI any information they did hold on this point because, they said, it would take too long to collate the data. This is because they store data in different places and different ways, with no clear or consistent approach to its collection or storage. Sometimes, the police store racial identity data in the PCMT, and sometimes in other databases; at the same time, sometimes the person inputting data into the relevant database includes racial identity within a pre-defined box for recording ethnicity, while on other occasions the enter it into ‘free text’ field. As a result, the data is not ‘searchable by automatic means’, and the government cannot aggregate it.<sup>200</sup>

If the government wanted to know the impact of Prevent on people from particular racial or religious groups, or people with disabilities, it would be organising and handling its data very differently. Instead, it is – in effect – choosing not to know.

The result is that the NPCC, which ostensibly manages the main Prevent database, cannot meaningfully assess any potential discriminatory impacts of Prevent: it does not have accurate data. Indeed, following RSI’s appeal to the Information Commissioner’s Office, the NPCC told us that it would take over five years’ worth of working days for it to collate the data it holds about the racial identity of people referred to Prevent.<sup>201</sup>

---

<sup>200</sup>Internal review of FOI 01/FOI/23/031840, 29 August 2023 (available at Annex J).

<sup>201</sup>Information Commissioner’s Office, [Decision Notice IC-262164-Z2K6](#), 20 December 2023, paras. 20-24.

This situation is not an accident: it is the result of choices about data collection and database architecture. Those are choices that the responsible officials could have made differently.

It is hard to justify the continued existence of inaccurate and non-comprehensive race data of people referred to Prevent, when there are government-designated best practices on the collection of racial identity data (such as the 18+1 categorisation) that the police and the Home Office use to assess the impact of their other policing and counter-terrorism programmes.

The police's failure to collect the data they need to conduct effective and accurate equality impact assessments is particularly unacceptable given recent findings and pervasive claims that police in the UK, including the Metropolitan Police (which have a major hand in Prevent), are institutionally racist, sexist or otherwise discriminatory.

For example, Baroness Casey, who led an official review into the Metropolitan Police force, concluded in 2023 that there is 'institutional racism, misogyny and homophobia in the Met'. Some of the details she described included:

*'Claims for disability discrimination is [sic] the most frequent claim type brought against the Met. But there is no willingness to learn from these cases.*

...

*There is deep seated homophobia within the Met, as shown by the fact that almost one in five lesbian, gay and bisexual Met employees have personally experienced homophobia and 30% of LGBTQ+ employees have said they had been bullied.*

*Trust, confidence and fairness scores among LGBTQ+ Londoners have fallen significantly.*

...

*Female officers and staff routinely face sexism and misogyny.*

...

*There are people in the Met with racist attitudes, and Black, Asian and ethnic minority officers and staff are more likely to experience racism, discrimination and bullying at their hands. Discrimination is often ignored, and complaints are likely to be turned against Black, Asian and ethnic minority officers. Many do not think it is worth reporting... Meanwhile Black Londoners in particular remain over-policed. They are more likely to be stopped and searched, handcuffed, batoned and Tasered, are overrepresented in many serious crimes, and when they are victims of crime, they are less satisfied with the service they receive than other Londoners. There is now generational mistrust of the police among Black Londoners. Stop and search is currently deployed by the Met at the cost of legitimacy, trust and, therefore, consent.'*<sup>202</sup>

While Baroness Casey's conclusions apply only to the Metropolitan Police, they are consistent with broader public concerns about a culture of discrimination within policing in general – concerns noted by the current Chair of the NPCC, Chief Constable Gavin Stephens.<sup>203</sup>

In 2022-2023, the police made 29 percent of all Prevent referrals, second only to referrals from the education sector.<sup>204</sup>

<sup>202</sup>Baroness Casey of Blackstock, 'An independent review into the standards of behaviour and internal culture of the Metropolitan Police Service: Final Report' (March 2023), pp. 16-17.

<sup>203</sup>National Police Chiefs' Council and College of Policing, 'Police Race Action Plan: Improving Policing for Black People' (NPCC, 2022).

<sup>204</sup>Home Office, 'Individuals referred to and supported through the Prevent Programme, April 2022 to March 2023' (14 December 2023), section 2.1. The police have accounted for a similar proportion of Prevent referrals since 2021: 28% in 2021-2022. See Home Office, 'Individuals referred to and supported through the Prevent Programme, April 2021 to March 2022' (26 January 2023), section 2.1.

We also know that the majority of police Prevent referrals come from the Metropolitan Police.<sup>205</sup> That is, a substantial portion of Prevent referrals are coming from a police force that an independent review has found to be institutionally racist and riddled with other problems of discrimination.

Given the well-documented risk that officials and others could be implementing Prevent in a discriminatory manner, with rights-violating outcomes for individuals (including children) and cumulative harms to groups such as British Muslims and children or adults of Black or Asian descent, much greater public information about how the Home Office, police and other public bodies gather and otherwise process data under Prevent – including data legally classified as sensitive – is vital.

The inconsistent and otherwise problematic storage of data about race under Prevent also raises questions as to whether these public bodies are complying with the public sector equality duty (PSED): the obligation on public bodies in the UK to have ‘due regard’ to their equality law obligations.<sup>206</sup> Such a legal violation could arise because Prevent-related data about race:

- a. Is not systematically stored;
- b. Is not stored in the same way for each instance of storage;
- c. Is stored in different ways by different public bodies;
- d. Is not subject to clear and specific guidance on when, why and how it should be collected and stored;

- e. Is not monitored for any disproportionate impacts on certain communities; and#
- f. Is defined by the case officer’s reporting of the individual’s racial identity, and not self-reporting (which would mean that any attempt to measure possible discrimination under the PSED would ‘almost certainly’ be inaccurate, to use the Home Office’s language).<sup>207</sup>

In a 2011 equality impact assessment for Prevent, the government noted the risk that activities under Prevent could have a discriminatory impact on certain groups – and said it would be necessary in future to collect data to monitor the potential disparate impacts of the strategy. Yet, it appears that data about race has not been collected in a way that would enable anyone to make such an assessment. While the updated August 2024 model Prevent Referral Form includes a distinct ‘ethnicity’ category, this is not in a drop-down box and there is no official guidance to suggest which categories referrers should use. In our analysis, this approach does not suggest there will be any improvement in the amount or (crucially) accuracy of the data collection.

Additionally, while the new model referral form notes that the person filling out the form should ‘only provide personal data if this information is already known from an official source or was provided by the person in question’, there remains a high risk of inaccurate and poor equality monitoring. First, we do not know how many entities use the model form. Second, as we discuss above and elsewhere, the government tells Prevent practitioners to avoid seeking consent to a referral in a wide range of instances

<sup>205</sup>Home Office, ‘Individuals referred to and supported through the Prevent Programme, April 2022 to March 2023’ (14 December 2023), ‘data tables’, Table 17.

<sup>206</sup>Including putting an end to behaviour which breaches the Equality Act 2010, advancing equal opportunities and fostering good relations: *Equality Act 2010*, s149. For a summary, see Equality and Human Rights Commission, ‘The Public Sector Equality Duty (PSED)’ (Equality and Human Rights Commission, 28 June 2022). For more information, see *The Equality Act 2010 (Specific Duties) Regulations 2011*, SI No. 2260.

<sup>207</sup>For a brief explanation of the PSED obligation see *R (Brown) v. Secretary of State for Work and Pensions* [2008] EWHC 3158; *R (on the application of Bracking and others) v. Secretary of State for Work and Pensions* [2013] EWCA Civ 1345; *R (Sheakh) v. London Borough of Lambeth* [2022] PTSR 1315; *R (on the application of Danning) v. Sedgemoor District Council* [2021] EWHC 1649 (Admin).



– meaning that referrers are unlikely to ask for the information from ‘the person in question’. Third, ‘official sources’ may themselves be inaccurate or not rely on self-reported information.

Alongside adequate data collection, good and effective equality monitoring also requires sufficient data and other analysis. For example, the Equality and Human Rights Commission – the non-departmental public body responsible for overseeing equality and non-discrimination legislation in England, Wales and Scotland – has published guidance for public bodies on how to monitor the equality impacts of their policies and programmes. In this guidance, it explains:

*‘You must collect evidence to monitor whether your policy is actually having an impact on people with particular protected characteristics. You should also collect evidence to monitor whether the actions you took to mitigate negative impact or maximise positive impact have had the intended effect.’<sup>208</sup>*

All of these factors from our research lead us to fear that neither the police nor the Home Office want to remove the risk of biased referrals of Muslims or people from other minoritised groups.

## Mission creep: turning Prevent into a surveillance programme

Throughout this report, we have shown evidence of a ‘mission creep’, with the police using Prevent to create secret dossiers about people’s religions, beliefs, opinions, relationships and identities – whether real or invented by the observer – at a large scale. We have also shown that police could then seek to ‘disrupt’ people, including children, on the basis of these factors. Moreover, people could face these potentially rights-violating consequences even if they are never actually referred to Prevent.

First, we have seen the expansion of the PCMT database to include ‘potential referrals’, contradicting government statements that only formal Prevent referrals are stored in the database. This expansion of the PCMT is troubling for several reasons. People referred to Prevent, regardless of how their case is disposed, are not being referred because anyone thinks they have committed a crime; additionally storing and sharing data in this way contributes to a practice of ‘data hoarding’ – collecting and storing data that is of no use to the police, with a view that it might somehow become relevant at an undefined point in time. As far as we are aware, this data about ‘potential’ referrals can be accessed by the immigration authorities and a range of other bodies that can have major consequences for people’s lives. (Based on the information we have at our disposal, there appears to be no practical distinction between ‘potential’ and actual referrals in terms of who can access this data.)

---

<sup>208</sup>Equality and Human Rights Commission, ‘[How to consider equality in policy making: A 10-step guide for public bodies in England](#)’ (updated 12 September 2024), Step 8. Similar guidance exists for public bodies in Scotland and Wales: Equality and Human Rights Commission, ‘[Assessing impact and the equality duty: an eight step guide](#)’ (updated 29 June 2020); Equality and Human Rights Commission, ‘[Assessing impact and the Equality Duty: A guide for listed public authorities in Wales](#)’ (updated 1 October 2014).



As well as its inherent privacy impacts, data hoarding could also impact the efficiency of decision-making processes by causing officers to become overwhelmed with useless or misleading data when they need to act quickly in response to an unfolding situation.<sup>209</sup> Further, algorithms – which are created by people – could produce ‘results’ based on this data that reflect and reinforce bias, or are simply wrong.

We are also concerned that the police may have broadened the PCMT’s remit so as to create a form of surveillance against particular groups or communities. On slide 7 of Counter Terrorism Policing’s PCMT training, the CTP explains that the ‘subject’ of a database entry can be an ‘[i]ndividual, [i]nstitution or [i]deology’.<sup>210</sup> While the PCMT is ostensibly a piece of case management software that the police should use solely for individual cases, it appears that the system also includes information about particular groups or – potentially – communities. This information is searchable and sharable. It appears that someone who has never been referred to Prevent themselves could still end up in the Prevent database because they have joined a certain student group or attend a certain mosque, for example. We recall that the government has previously accused entire schools of being ‘Trojan horses’ for Islamism,<sup>211</sup> and even if it would not do the same under its current leadership, the risk remains that police will secretly decide that an entire school or house of worship is suspect—or everyone who visits a certain website or buys a certain book.

On the other hand, we also know from prior freedom-of-information requests made by others that some Prevent data is deliberately excluded from the PCMT, and instead entered into policing systems for ‘intelligence’ marked as ‘secret’.<sup>212</sup> We do not know what these databases are. The storage of Prevent data as ‘intelligence’ is a further example of how personal data related to a Prevent referral could have a lingering impact – engendering suspicion of the person, including a child, and unknown future consequences.

Many of the troubling data practices we see regarding the PCMT are also reflected in the police’s use of PLPs. Given the ambiguous restrictions surrounding the storage and sharing of PLP data, coupled with the potentially broad range of government agencies involved and types of data stored, we are confronted with a situation in which PLPs apparently have expansive surveillance powers and near limitless use of a referred person’s sensitive data, to the point of being able to share that data with foreign governments.

On top of the PCMT and PLP, we see data hoarding within the PNC. Campaigners have criticised how the police store data on the PNC in general, while some data collection and retention practices diverge between different forces. For instance, an investigation published in August 2023 by OpenDemocracy, an investigative journalism organisation, found that many UK police forces are likely holding biometric and surveillance-related data unlawfully ‘in part because their ageing computer systems don’t allow them to delete data entries in bulk.’

---

<sup>209</sup>See, e.g. Samuel Woodhams, ‘[A secretive Home Office unit has hoarded data on millions of people](#)’ (Wired, 7 April 2021); Jessica Lyons Hardcastle, ‘[Privacy watchdog steps up fight against Europol’s hoarding of personal data](#)’ (The Register, 23 September 2022).

<sup>210</sup>Document Number NCTPHQ/ICT/215, 31 May 2018 (available at Annex D).

<sup>211</sup>See HM Government, ‘[Government Response to the Education Select Committee Report: Extremism in schools: the Trojan Horse Affair](#)’, Cm 9094 (July 2015). See, further, John Holmwood and Therese O’Toole, [Countering Extremism in British Schools? The Truth about the Birmingham Trojan Horse Affair](#) (Bristol: Bristol University Press, 2017).

<sup>212</sup>Metropolitan Police Service, ‘[CTP Prevent Policy 2020](#)’, released under 01.FOI.21.021978, p. 9.

The same investigation found that some forces have created 'blanket retention' policies for all DNA samples, while others systematically used the Immigration and Asylum Biometrics System to check the immigration status of people with whom they engage.<sup>213</sup> In other words, the storage of Prevent data on the PNC is taking place in the context of broader, allegedly illegal practices.

The extensive scope of the data collection raises concerns about whether it is driven by necessity or simply for the (supposed) convenience of having an extensive surveillance system. If the police and the government think the status quo is merely 'convenient', then this raises questions about the government's compliance with Article 8 ECHR.

## Avoiding consent

'Consent' is not actually consent if the police are going to intervene anyway. We have seen how the police, if they decide they do not want to ask for consent to a Prevent or Channel referral (or the individual refuses), may instigate a PLP instead.

This practice raises questions about whether any consent to Prevent or Channel is truly informed or valid, and in turn whether the UK is complying with data protection law.<sup>214</sup> As we explained in *Secret, Confused and Illegal*, despite describing Prevent as a consensual programme, the government's guidance often tells practitioners to refer people without obtaining the person's consent.<sup>215</sup>

Similarly, the Government Legal Department, on behalf of the Home Office, told us that that 'persons referred to Prevent are not generally made aware of their referral unless they are invited to participate in the Channel programme'.<sup>216</sup> Such statements and practices lead us to the conclusion that Prevent is not a consensual programme.

Even if a practitioner seeks the person's consent when they are engaging them in the Prevent process, the broad and secretive data sharing and storage we have outlined here would significantly go beyond any consent an individual would have granted. People cannot 'consent' to things they do not know about.

For instance, in Kirklees Council's Prevent guidance for professionals subject to the Prevent duty, it states:

*'Following a referral, the information received is assessed by the Police. Following this assessment a decision will be made on the suitability of the case for discussion at the Kirklees Channel Panel. If the case is not suitable for Channel the Police will notify the referrer about the outcome of the assessment and if necessary make a referral to other agencies for support. Following assessment, if the case is deemed suitable for Channel support then the referrer will be invited to the next Channel Panel meeting. The referrer should continue to monitor the case and keep Prevent updated with any additional information which could lead to an increase in vulnerabilities to radicalisation.'*<sup>217</sup>

---

<sup>213</sup>Mark Wilding and Anita Mureithi, '[Police are unlawfully storing personal data of suspects who were cleared](#)' (OpenDemocracy, 17 August 2023).

<sup>214</sup>For a summary, see ICO, '[Consent](#)' (ICO, no date).

<sup>215</sup>Rights & Security International, '[Secret, Confused and Illegal: How the UK Handles Personal Data Under Prevent](#)' (2022), paras. 11, 31-35, 41-44, 49-50, 57-59, 126.

<sup>216</sup>Government Legal Department, communication with RSI on behalf of the Home Office, ref no. Z2409530/CB4/DS4, 17 September 2024, para. 5.

<sup>217</sup>Kirklees Prevent, '[Channel Referral Guidance for Partners](#)' (2018), p. 7.

While this guidance tells professionals that Prevent data will be shared with the police, Channel and potentially other support agencies (depending on the outcome of the Channel panel), it says nothing about – for example – the immigration authorities, MI5, MI6 or foreign governments. If the person instigating a referral does not know about this broad data-sharing, how could they ask the person being referred for consent to it? (Moreover – we must ask – who would freely say ‘yes’?)

In terms of consent, we also should be aware that UK data protection law provides some authority to children to consent to their data processing. In contrast to the approach data protection law takes to children accessing online services (for which children under the age of 13 cannot lawfully consent),<sup>218</sup> the approach for other forms of data processing and sharing depends on whether the child has the mental capacity to consent.<sup>219</sup> It is unclear to us how the police decide whether to approach the child or their parents to ask for consent – the government’s and the Metropolitan Police’s data privacy notices do not address this.<sup>220</sup> Regardless, if adults do not fully understand how the police use data about a Prevent referral or the Channel process, neither will children.

## Final comments

In the year ending March 2023, there were 6,817 Prevent referrals. Among these, 2,684 students, parents or teachers were referred by schools. More than 2,000 were aged 14 or under.<sup>221</sup> Each of these people – mostly children<sup>222</sup> – have had personal information stored about them on police databases used to monitor what they believe and what they say. In many cases, that information will be accessible to the immigration authorities. At the same time, the police couple this information with sensitive data about who these children or adults are, and whom they might know, to form an ‘intelligence’ picture – in some cases potentially even going so far as trying to ‘disrupt’ them.

But we only get part of the picture by looking at the government’s statistics on referrals. Alongside data of people referred to Prevent, police databases also store information about ‘potential referrals’, meaning that should a school or hospital contact the police to get advice about how to engage with a student or patient, the police will also store and share this data. All of this happens without the caller knowing.

Simply put, Prevent is a vast secret surveillance and intelligence programme – one that mainly affects children. The way police and other authorities treat people’s, including children’s, private information under the programme breaches the law. It is not possible to have a programme that involves capturing and widely sharing information about thousands of people’s race, religion, belief, opinion, disability or sexuality and that also complies with the European Convention on Human Rights. **The UK government must end Prevent.**

---

<sup>221</sup>Home Office, ‘Individuals referred to and supported through the Prevent Programme, April 2022 to March 2023’ (14 December 2023).

<sup>222</sup>The most recent statistics show that 63% of referrals in which the age of the individual is known involves people aged 20 or under: Home Office, ‘Individuals referred to and supported through the Prevent Programme, April 2022 to March 2023’ (14 December 2023).

# Recommendations

In light of the findings of this report, the UK government should:

- 1 End Prevent, as it is not possible to have a programme of this nature that complies with data protection or other human rights. Prevent entails the government's collection and storage of information about people's (mainly children's and young people's) race, national origin, religion or belief, political or other opinion, thought, gender or gender identity, health, sexual practices, disability status and/or other sensitive aspects of personal life and identity – on a massive scale, and overwhelmingly in secret. It is not possible to carry out these activities in compliance with the Human Rights Act or the European Convention on Human Rights, and some may also violate UK data protection law.
- 2 Stop treating children as potential 'terrorists' and ensure full compliance with the Convention on the Rights of the Child when it comes to children's and parents' interactions with police, the justice system, schools, social services and the health care sector.
- 3 Reform police data management systems and practices so that any safeguarding data police hold is not treated as 'intelligence' and not shared with intelligence agencies, whether UK or foreign.
- 4 Publish a complete map of Prevent data flows and ensure that the authorities provide this to everyone before asking them to consent to participate in Prevent or Channel – or consent to allow their children to participate, as applicable.
- 5 Publish aggregated data about the racial identity of people referred to Prevent via annual statistical releases, as well as data showing the intersection between race and the outcome of the referral process. Do the same regarding Channel.
- 6 Similarly, publish aggregated data about the religion and disability status of people referred to Prevent and/or Channel, along with data showing the intersection between race and the outcome of those processes.
- 7 Ensure that all government bodies delete all Prevent- and Channel-related data within a predetermined number of years – one that cannot be increased to allow de facto indefinite or lifelong retention.
- 8 Otherwise ensure that all laws and guidance comply with human rights and data protection laws.

# Recommendations

## Police in the UK should:

- 1 Stop using their powers (including 'disruptive' powers) against people who are not inciting violence or discrimination, or otherwise committing a criminal offence.
- 2 Reform their data management systems and practices so that any safeguarding data they hold is not used for 'intelligence' and there is clarity and transparency regarding how and when they collect people's personal data.
- 3 Ensure that they operate Channel – if at all – as a truly consensual process, without skirting consent requirements. This would mean, inter alia, ending secretive Police-Led Partnerships.
- 4 Explain who has access to Prevent data and provide a map of all Prevent data flows.
- 5 Comply with government best practices about the collection of racial data, including using the 18+1 or 19+1 race/ethnicity categories for Prevent and Channel, and by relying on the individual's self-reporting of their identity.
- 6 Commit to, and carry out, high-quality equality impact monitoring of Prevent and Channel, and publish regular reports on this topic.
- 7 Otherwise ensure that guidance complies with human rights and data protection laws.

***We call on public bodies subject to the 'Prevent duty' to educate Prevent leads and other staff on how the police and other authorities may use Prevent data, including where this data goes and how a referral could impact a person's life.***

# Acknowledgements

Jacob Smith, RSI's UK Accountability Team Leader, researched and drafted this report. Josephine Dumbrell, Digital and Privacy Rights Assistant, and interns Eleanor Farah and Asher Miller provided additional research and drafting support. Sarah St Vincent, Executive Director, reviewed the report and Communications Officer Renee Karunungan formatted and published it.