Secret, Confused and Illegal: How the UK Handles Personal Data Under Prevent

RIGHTS & SECURITY INTERNATIONAL

Visit us at www.rightsandsecurity.org
and follow our work on Twitter @rightssecurity

Contents

1. Summary

1. The UK government, through its controversial Prevent strategy, says it aims to stop people from being 'drawn into terrorism'. Many high-profile reports by journalists and charities have pointed to negative impacts the strategy has had, particularly on Muslim communities, since its inception. We know from these and other sources that government authorities process – by collecting, using, storing, or sharing – people's personal data when implementing Prevent; however, little research has been conducted on these practices to date.

2. This report explains what we know about how people's personal information is shared under Prevent, and analyses whether these practices follow human rights and data protection laws.

3. We conclude that the UK's current practices are secretive, confused, and – under the European Convention on Human Rights (ECHR) – illegal.

4. **Secret:** Prevent, like other aspects of the government's national security strategy, operates largely in secrecy. The handling of people's personal data under Prevent is no exception. We conclude that, despite an abundance of general government guidance about Prevent, little information exists about how the government believes agencies such as police, schools, hospitals and local authorities should treat people's personal information under Prevent.

5. Many individual agencies are just as secretive, often having no publicly available Prevent policy, let alone one that outlines the circumstances in which the agency uses Prevent-related personal data.

6. **Confused:** The government's Prevent policies are also confused, failing to explain clearly how agencies that handle people's personal information – from universities to mental health professionals – should treat data that could be relevant to Prevent. While occasionally mentioning human rights and data protection norms, the government does not advise strict respect for people's rights. Instead, it suggests that professionals, police and schools should prioritise gathering, storing and sharing Prevent-related data.

7. There are also examples of inconsistent practices and advice within specific fields. For instance, we find that different professional organisations in the medical sector advise their members to act in different ways when it comes to handling Prevent-related data. On top of this, National Health Service (NHS) guidance diverges from what the professional organisations say.

8. **Illegal:** We conclude that the UK's handling of personal data under Prevent is illegal under the ECHR. At minimum, the treatment of personal data under Prevent is not based on clear and accessible laws and regulations regarding how government bodies may gather, store, share and otherwise process the data, violating Article 8 of the Convention. We state these views about illegality only regarding the UK government

as a whole, and not any specific agencies, local authorities, NHS trusts or non-government bodies.

9. The ways personal information is handled under Prevent may violate the law for other reasons as well.

10. Under Article 8 of the ECHR, the UK government is obliged to uphold everyone's right to respect for their private and family life. This includes an obligation not to collect, store or otherwise process private information (generally including many types of personal data) about an individual except where this is specifically allowed by law and necessary to achieving a legitimate goal. Laws allowing the collection and handling of people's private information must be clear and accessible, and explain the circumstances in which the government or other institutions can process the personal data. We conclude that UK's current laws and practices violate this 'legality' requirement found in the ECHR, including because the existing laws and policies are not sufficiently clear or specific, while in many instances the relevant guidelines and policies are not even publicly available.

11. The UK's handling of private information under Prevent will also violate this 'legality' element of Article 8 of the ECHR if it violates the country's own laws. In general, UK data protection laws provide that any gathering, storage or sharing of personal data will only be legal if the person has consented or if there is some other specific authorisation for the data collection and handling. If the person has consented, this consent must be free, voluntary and informed, meaning that the person must be capable of refusing and informed about how the data will be used, and cannot be forced to say yes. In the Prevent context, our research raises concerns about non-consensual data processing, with the government and public bodies frequently advising practitioners to avoid seeking consent before processing personal data. This has led to many situations in which an individual is likely unaware that their personal data could used for a range of purposes, or that an authority still holds Prevent-related data about them. If the data collection and handling does not have some other valid basis in the law, it would be illegal.

12. It is true that under UK law, permissible grounds for data processing (other than consent) are broad; among other activities, they could allow the receipt and handling of Prevent data by the intelligence agencies, potentially on a massive scale. However, this does not change our conclusion that data processing practices under Prevent likely breach UK data protection laws (and therefore the ECHR), particularly since data is processed in secret and apparently without sufficient oversight. Additionally, many authorities appear to store this data for longer than is necessary.

13. For clarity, we observe that the UK's handling of people's private information under Prevent can violate the ECHR (see above) even if the authorities are not breaking UK data protection laws.

14. We also conclude that the government has failed to prove that its collection and other processing of people's personal information under Prevent are genuinely necessary to

achieving the goal of stopping terrorism. This violates the 'necessity' requirement of Article 8 of the ECHR.

2. Introduction

15. The long-controversial 'Prevent' strategy is a UK government programme with the stated goal of 'prevent[ing] people from being drawn into terrorism', and is often described as a strategy to prevent or counter violent extremism (P/CVE).[1] It forms one part of the UK's broader counter-terrorism strategy, CONTEST, which the then-Labour government introduced in 2005 – partly in response to the 7 July bombings in London.[2]

16. Successive governments have developed Prevent significantly over the past two decades. Professor Paul Thomas, Associate Dean of Research Innovation and Knowledge Exchange at the University of Huddersfield, has identified three distinct iterations of Prevent: 'Prevent 1', focusing primarily on engaging directly with Muslim communities (2006-2011); 'Prevent 2', re-orienting Prevent to end its community focus, instead seeking to identify vulnerable *individuals* 'at risk' of 'radicalisation'; and 'Prevent 3', following the introduction of the statutory Prevent duty, discussed below.[3]

17. When the police or another public authority refers an individual for Prevent intervention[4] – that is, when they decide they believe the person could be at risk of being drawn into terrorism – the referral then proceeds through the 'Channel' process, whereby safeguarding professionals meet to determine whether the person requires any further intervention (see Figure 1). If the Channel panel adopts the case, it will subsequently meet at least monthly to discuss this and other ongoing cases.[5] The Home Office's Channel guidance states:

    'Each case is handled separately. People deemed appropriate to receive support will have a tailored package developed for them, according to their identified vulnerabilities. Using the initial vulnerability assessment and their professional expertise, the panel should develop a package to support the needs of the individual and use the information to inform the assessment and mitigation of any risk posed to potential support providers.'[6]

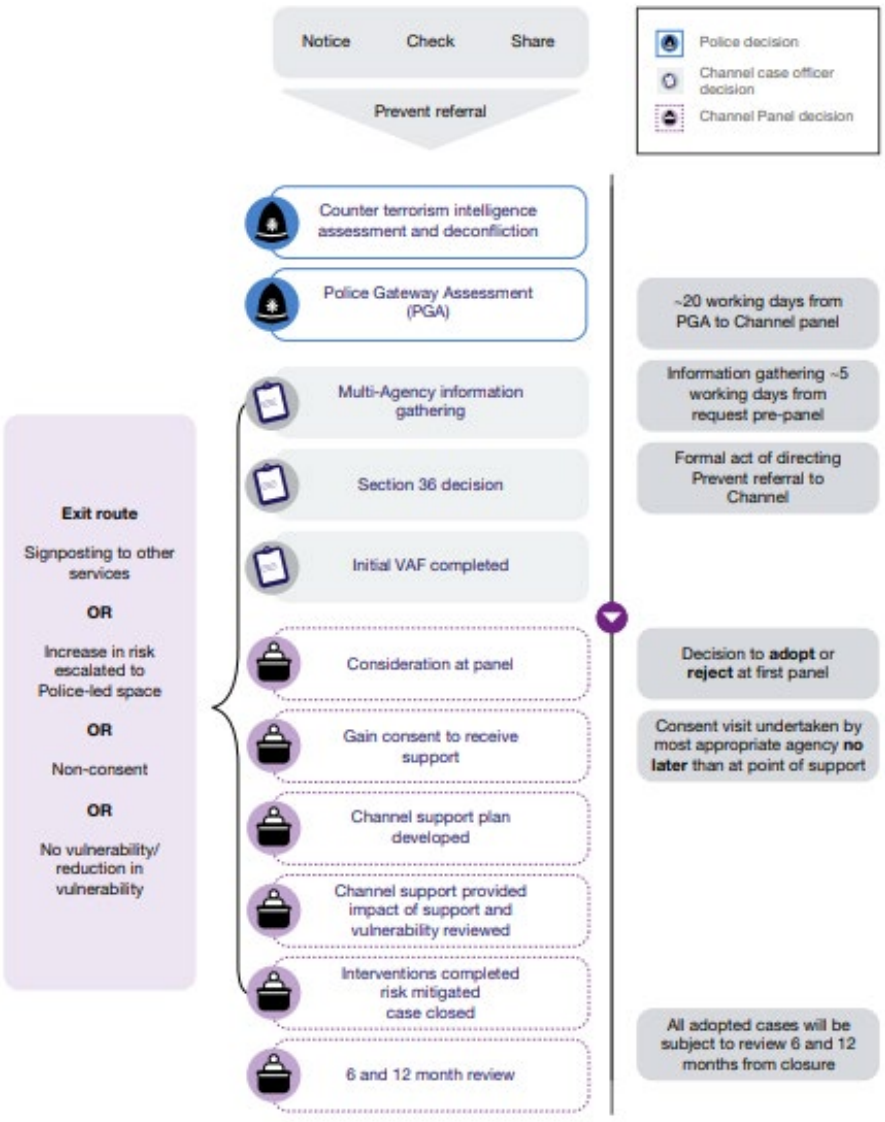
---

[1] Home Office, 'Prevent duty guidance: for further education institutions in England and Wales' (*Gov.uk*, 1 April 2021).
[2] Jay Edwards and Benoît Gomis, 'Islamic Terrorism in the UK since 9/11: Reassessing the 'Soft' Response', International Security Programme Paper – ISP PP 2011/03 (*Chatham House*, June 2011), pp. 4-5.
[3] Paul Thomas, 'Changing experiences of responsibilisation and contestation within counter-terrorism policies: the British Prevent experience' (2017) 45(3) Policy and Politics 305.
[4] The police may also receive referrals from members of the public, or other public authorities which are not empowered to instigate the Prevent process themselves. In such circumstances, the police may determine to refer a case for Channel intervention: see Table A and accompanying footnotes for more information.
[5] HM Government, 'Channel Duty Guidance: Protecting people vulnerable to being drawn into terrorism' (2020), section 6.
[6] HM Government, 'Channel Duty Guidance: Protecting people vulnerable to being drawn into terrorism' (2020), para. 107.

Regardless of the outcome of the Channel process, the panel can decide to forward the individual's case to other professionals, such as the mental health services, for additional or alternative support.[7]

18. In the period from April 2020 to March 2021 (the most recent for which statistics are available), there were 4,915 referrals to Prevent,[8] of which the Channel panel considered 1,333 and adopted 688 as cases.[9]

Figure 1: Channel pathway diagram[10]



[7] Further, see Counter-Terrorism and Security Act 2015, s36(4).
[8] Although this figure was likely impacted by the Covid-19 pandemic; in the year ending March 2019, authorities referred 5,738 individuals to the Prevent programme in England and Wales: see Home Office, 'Individuals referred to and supported through the *Prevent* programme, England and Wales, April 2018 to March 2019' (*Gov.uk*, 19 December 2019).
[9] Home Office, 'Official Statistics: Individuals referred to and supported through the Prevent Programme, April 2020 to March 2021' (*Gov.uk*, 18 November 2021).
[10] Reproduced from HM Government, 'Channel Duty Guidance: Protecting people vulnerable to being drawn into terrorism' (2020), p. 21.

Human rights experts, community groups, and academics have criticised the strategy since its inception for its impacts on Muslim communities.

19. Human rights experts, community groups, and academics have criticised the strategy since its inception for its impacts on Muslim communities. For instance, Prevent has reportedly limited the willingness or ability of Muslims in Britain to engage with legitimate academic and other debates, and authorities have reportedly treated Muslims as 'suspect communities'.[11]

20. While the strategy's initially stated focus was solely on preventing 'extremism' that the government associates with Islam, the Home Office expanded the mandate in 2011 to add other forms of 'extremism', most notably beliefs associated with the far right.

21. However, despite this shift, many commentators continue to criticise Prevent on the grounds that, in implementing the strategy, authorities still disproportionately target Muslim communities – even though the percentage of initial referrals leading to subsequent intervention for people who have, or may have, Islamic beliefs is significantly lower than for other demographics.[12]

22. This marginalisation of Muslim communities through Prevent has accompanied additional limits on broader civil society under the strategy, through which – as RSI and others have reported – the authorities can directly discourage activists from participating in democracy, education or the arts, or create an atmosphere of fear that has the same effect.[13]

23. Counter-terrorism and human rights experts have also criticised Prevent for its gendered impacts, particularly oversimplification and stereotyping of the role of women in society and a disproportionate focus on engaging with women from middle class

---

[11] The phrase 'suspect communities' was first promulgated by Paddy Hillyard to categorise the UK government's response to the conflict in Northern Ireland: see Paddy Hillyard, *Suspect Community: People's Experience of the Prevention of Terrorism Acts in Britain* (London: Pluto Press, 1993). For an overview of the phrase's application to Muslim communities, see Christina Pantazis and Simon Pemberton, 'From the 'old' to the 'new' suspect community: Examining the impacts of recent UK counter-terrorist legislation' (2009) 49(5) Criminology and the War on Terror 646. For the impact on Muslim communities generally, see Tahir Abbas, Imran Awan and Jonathan Marsden, '*Pushed to the edge*: the consequences of the 'Prevent Duty' in de-radicalising pre-crime thought among British Muslim university students' (2021) Race, Ethnicity and Education 1; Tufyal Choudhury and Helen Fenwick, 'The impact of counter-terrorism measures on Muslim communities' (Equality and Human Rights Commission, 2011); Miqdaad Versi, 'Meeting between David Anderson QC and the MCB: Concerns on Prevent' (The Muslim Council of Britain, July 2015); Sariya Cheruvallil-Contractor, 'Government policy has left Muslim students feeling unable to speak up on campus' (*The Conversation*, 15 July 2020); Jamie Grierson, 'Hundreds of Islamic groups boycott Prevent review over choice of chair' (*The Guardian*, 17 March 2021).

[12] From April 2020 to March 2021, Channel panels adopted 22% of cases involving alleged Islamic radicalisation as a case, compared to 46% of cases involving alleged right-wing extremism: see Home Office, 'Official Statistics: Individuals referred to and supported through the Prevent Programme, England and Wales, April 2020 to March 2021' (*Gov.uk*, 18 November 2021).

[13] Zin Derfoufi and Rights & Security International, '*Prevent*-ing Dissent: How the U.K.'s counterterrorism strategy is eroding democracy' (2022).

backgrounds, while limiting engagement with women who express concerns about how Prevent works.[14]

24. RSI believes any analysis of the use of personal data under Prevent should take place with these factors in mind, particularly as gender, race and religious beliefs are all types of personal data collected as part of Prevent.

25. This report includes three parts. First, we gather and summarise publicly available information – such as policies and trainings – about how authorities, schools, doctors and others should handle Prevent-related data about people. Second, we analyse this material – concluding that the government may be pressuring practitioners to engage in over-cautious data storage and sharing, without clear laws or enough attention to human rights and data protection considerations. Finally, we assess these practices under domestic and international human rights and data protection laws, before concluding that the government, under the current approach, is breaking the rules.

[14] Katherine E. Brown, 'Gender, governance, and countering violent extremism (CVE) in the UK' (2019) International Journal of Law, Crime and Justice 1, pp. 4-8; Narzanin Massoumi, ''The Muslim woman activist': Solidarity across difference in the movement against the 'War on Terror'' (2015) 15(5) Ethnicities 715. This may also extend from general perceptions of the role of women by the police: see John Bahadur Lamb, 'Gendered counter terrorism? The potential impact of police officer perceptions of PREVENT policing' (2014) 6(3) Behavioral Sciences of Terrorism and Political Aggression 183, pp. 183-185. On the international level, see Ann Kathrin Rothermel, 'Gender in the United Nations' agenda on Preventing and Countering Violent Extremism' (2020) 22(5) International Feminist Journal of Politics 720; Fionnuala Ní Aoláin and Jayne Huckerby, 'Gendering Counterterrorism: How to, and How Not to' (*Just Security*, 1 May 2018).

Person X: Our hypothetical example

The operation of Prevent remains secretive, and the laws on privacy and data protection can also be highly technical. Therefore, we have created the following fictional example to help explain why these technical points are important for the lived experiences of real people in the UK.

This case study is hypothetical, but is based on real reported experiences with Prevent.[1]

Person X was born in the UK to a Muslim family, and they are now studying politics at a UK university. As part of their extra-curricular activities, Person X decides to join some university societies, including one that holds debates and another that peacefully advocates for human rights. As part of their community and society work, Person X has started voicing concerns about Prevent, especially its impact on Muslim communities. Recently, Person X submitted an essay on the Prevent strategy, receiving a distinction. The essay included critiques of government policy but expressed no desire or plans for violence.

A member of teaching staff (Dr Y) has become concerned that Person X may be exhibiting 'extremist' behaviours. This member of teaching staff is aware of Person X's extra-curricular activities with university societies and their local Muslim community, and the recent essay on Prevent has heightened their concerns.

Dr Y and the university's Prevent lead have completed trainings on Prevent from the university, the Home Office and the Department for Education (DfE), and they have reviewed the associated guidance. Both the professor and this university administrator have been trained on what the government thinks the signs of 'extremism' or 'radicalisation' are, and on the requirement to make a referral when they are concerned that someone is being drawn into terrorism.

Dr Y discusses the case with the administrator (the university's Prevent lead), before referring the case to the formal Prevent process (see Figure 1). They find this decision difficult, mainly due to conflicting guidance. Ultimately, however, the university instigates the formal Prevent process without informing Person X.

Person X only becomes aware of the Prevent referral when specialist police officers appear at their home the following week – an experience that feels intrusive and intimidating. Following the visit, the police decide not to refer the case to the official Channel process.

Although everyone involved recognises that the referral was a mistake, the police decide to retain the information from the referral – including Person X's name, age and ethnicity, as well as information about their family and religious beliefs, health and the reason for the referral – on their dedicated Police Case Management Tracker (PCMT), a database. The university also keeps a file with the same information, in line with its secret Prevent policy (which neither Person X nor the general public is aware of). Neither the police nor the university tells Person X about this storage of their personal information. By policy, each body stores Prevent-related data for an initial period of three years, with the possibility of an extension every 12 months afterward.

Person X continues with their studies but feels upset, intimidated and spied-on. They stop going to class and drop out of the student groups, even though they could have had leadership roles. They also start avoiding any unnecessary contact with their professors or university staff, including mental health support. They manage to graduate, but their grades have suffered. Once, they apply for a job in the civil service and get an offer, but the offer is then rescinded because a background check brings up the Prevent referral. When Person X applies for other jobs and asks the university for a reference, university staff are afraid to agree, because they can see the Prevent referral in Person X's file. Person X begins to lose hope that their life will improve, is fearful of the authorities, and becomes increasingly withdrawn.

3. What we know about data processing under Prevent

26. UK authorities can use many different types of data, or share it within and outside the government, when they act under Prevent. First, there is the information regarding the Prevent referral itself: the reason for the referral, who referred the person, and what (if any) follow-up action a Channel panel has taken. A range of actors may then process (handle) this data, and may store it for a length of time. Additionally, public authorities may record or share the individual's personal data – including their name, age, address and religion – as part of the Prevent process. We also know that some UK authorities share or use this personal information for non-Prevent purposes, such as policing.

27. Many public authorities – including local councils, education providers and NHS trusts – are also subject to the Prevent duty, which is the obligation to have 'due regard to the need to prevent people from being drawn into terrorism' in fulfilling their functions. To comply with this requirement, authorities must train individual practitioners in how to interact with the Prevent process, and the Home Office holds powers to enforce compliance with the duty.[15] As a result, practitioners and authorities may process personal data about people they refer for interventions. This 'Prevent duty' only applies in England, Wales and Scotland; it does not apply in Northern Ireland.

28. The government, in the multi-agency approach of the Prevent process, authorises the sharing of an individual's personal data by and across a number of bodies; once a member of the public or a professional[16] raises a concern that the person may need an intervention under Prevent, the relevant Prevent lead – for example, at a school or hospital – will consider the case and decide if the referring authority should escalate the case to the local police or to a Channel panel review (see Figure 1).[17] The referring authority then stores the individual's personal data, including biographical information, in the relevant Prevent database[18] – even if the referral is erroneous or the case did not escalate to the panel for evaluation – and then to the Channel panel for intervention.[19]

29. After this process, many other public bodies – such as the Home Office, education providers, the security services and the police – can access Prevent-related information in certain circumstances. While not the focus of this report, it also appears

[15] Counter-Terrorism and Security Act 2015, s26 (general duty on specified authorities), s30 (power to give directions), Schedule 6 (specified authorities).
[16] Predominantly individuals working in law enforcement, education, or the medical and social work fields.
[17] The route followed depends on whether the body has the statutory power to refer a case directly to the Channel panel, or whether they must instead refer the case to the police.
[18] 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), the High Court noted that *'the data [stored in relation to the Prevent referral] could be accessed by MPS officers, counter-terrorism officers nationally, local authorities… across 10 databases'* (at para. 77).
[19] For an overview of how the police engage in the referral process, see Chief Superintendent Nik Adams, 'Prevent: how we safeguard the vulnerable and how we manage our data' (*National Police Chiefs' Council*, 2019).

likely – as indicated in official government guidance – that the Home Office and other UK authorities may also share personal data with other countries.[20]

30. Many public (that is, government) and private bodies play a role in Prevent, and could come into contact with Prevent-related personal data as part of their functions. See Table A below for more information about the obligations and roles of each of these actors.

Table A: Actors with functions under Prevent that could process Prevent-related personal data

Actor	Representative examples	Functions[21]
Channel panel members[22]	Channel case officer; representatives from different safeguarding areas, including health, education and the police	Reviewing available data to determine whether an individual requires help and support; referring an individual to additional services, if deemed necessary[23]
Home Office	Home Secretary; Extremism Analysis Unit researchers; civil servants	Creating secondary legislation and official guidance on the operation of Prevent;[24] monitoring trends and conducting research and analysis for policy and operational partners;[25] directing authorities to act that may otherwise fail to fulfil their legal obligations;[26] funding civil society organisations working on P/CVE[27]

[20] HM Government, 'Counter-Extremism Strategy', Cm 9148 (October 2015), para. 42. Cross-border data sharing has become an increasingly prevalent phenomenon: see App. Nos. 58170/13, 62322/14 and 24960/15, *Big Brother Watch and others v. the United Kingdom*, Judgment, 25 May 2021, paras. 322-323.

[21] The term 'functions' is used here as some of the powers noted in the table are legal obligations, whereas others are not.

[22] For further information, see Home Office, 'Counter-Terrorism and Border Security Act 2019: Prevent and Channel panel Measures Fact Sheet' (2019); HM Government, 'Channel Duty Guidance: Protecting people vulnerable to being drawn into terrorism' (2020); Home Office, 'Case Study: The Channel programme' (*Gov.uk*, 13 December 2018).

[23] For more information on the Channel process, see Figure 1.

[24] Counter-Terrorism and Security Act 2015, ss27, 29, 36(7), 38(6), 39. In England and Wales, see HM Government, 'Channel Duty Guidance: Protecting people vulnerable to being drawn into terrorism' (2020).

[25] Question by Lord Hylton to the Home Office, 'Extremism Analysis Unit', UIN HL12796, tabled 14 January 2019, answered 28 January 2019.

[26] Counter-Terrorism and Security Act 2015, s30, 33.

[27] Ministry of Housing, Communities & Local Government, 'FOI release: Prevent funding' (*Gov.uk*, 7 July 2011). Prevent-related funding also has an international dimension: see Cabinet Office, 'Conflict, Stability and Security Fund' (*Gov.uk*, 15 December 2021).

Police services[28]	Chief Constables; British Transport Police; police and crime commissioners	Subject to the 'Prevent duty';[29] referring an individual to Channel;[30] collaborating with other public bodies in relation to a referral, including in conducting a 'gateway assessment' (see Figure 1)
Other public bodies	NHS Trusts; local authorities; schools; higher education institutions	Subject to the 'Prevent duty'; referring an individual to Channel;[31] collaborating with other public bodies in relation to a referral; funding civil society organisations working on P/CVE[32]
Civil society organisations	Faith leaders; community groups; voluntary organisations	Entering into contractual agreements with other authorities listed in this table for the purposes of implementing Prevent
Monitoring bodies	Ofsted; Office for Students; Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services; Home Secretary[33]	Monitoring compliance with Prevent; some also have the powers to sanction bodies or individual members for non-compliance
Professional membership bodies	General Medical Council; British Medical Association; National Police Chiefs' Council; College of Policing	Creating guidance (which may be statutory); guidance may also be binding on members through the organisation's membership rules
Practitioners	Doctors; teachers; social workers; police officers	Practitioners themselves are not under a legal duty to comply with Prevent, rather the body they work for is. They are obliged to follow any professional guidance

Consent to data processing

Many, if not most, people referred to Prevent do not explicitly consent to the authorities receiving and processing personal information about them for Prevent purposes. The concept of consent is crucial to data protection and privacy laws in the UK and around the world.

[28] For more information, 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).
[29] Counter-Terrorism and Security Act 2015, s26.
[30] Counter-Terrorism and Security Act 2015, s36.
[31] Counter-Terrorism and Border Security Act 2019, s20.
[32] Information on how local authorities distribute this funding is only sporadically available: see Derby City Council, 'Home Office funding to help prevention of radicalisation across England and Wales' (*Derby City Council*, 13 December 2021); Tower Hamlets Council, 'Prevent' (*Tower Hamlets Council*, 2021).
[33] Counter-Terrorism and Security Act 2015, ss30, 32(7), 33.

31. Many, if not most, people referred to Prevent do not explicitly consent to the authorities receiving and processing personal information about them for Prevent purposes.

32. The concept of consent is crucial to data protection and privacy laws in the UK and around the world. Under these laws, consent is not always required; additionally, in other areas of the law, courts will sometimes accept that consent is 'implied' even if the 'yes' was not explicit. However, as discussed below, the idea that consent should be obtained and must be explicit – that is, clear, specific and informed – is increasingly central in data protection laws. In any event, the question of who has consented, and what exactly they agreed to, is a critical one when it comes to data collection, storage and sharing. If a person has not consented, the authorities will need to be able to point to some other legal basis for gathering and sharing that person's data.

33. In the Prevent context, the referring authority often does not ask the referred individual for their consent to data sharing and collection relating to the initial referral. However, as Figure 1 demonstrates, the later Channel process operates differently. The government describes this process as voluntary, with the individual's consent being a pre-requisite for engagement with the process. Statutory Home Office guidance explains that that:

    'Consent to receive support should take the form of a signed agreement to support the auditable decisions of the panel and secured no later than at the point of offering support.'[34]

34. However, the reference to 'and secured no later than at the point of offering support' advises Channel panel members that they may process the individual's data while considering the case prior to seeking informed consent. In such instances, the panel will not directly notify the individual of the gathering, storage or sharing of their personal data.[35] Many people may therefore be unaware of the processing of their personal data under Prevent – indeed, this has meant that people referred to the Prevent process only become aware of the data processing several years later, or not at all.[36]

The government often assures practitioners who use Prevent-related personal data that consent is not required – in many instances even advising them to *avoid* seeking consent.

35. As this report discusses below, the government often assures practitioners who use Prevent-related personal data that consent is not required for data processing under Prevent – in many instances even advising them to *avoid* seeking consent before engaging in such data processing.

---

[34] HM Government, 'Channel Duty Guidance: Protecting people vulnerable to being drawn into terrorism' (2020), para. 119.
[35] HM Government, 'Channel Duty Guidance: Protecting people vulnerable to being drawn into terrorism' (2020), para. 123.
[36] As occurred 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), discussed further below.

Data storage

36. Public authorities use several databases for storing Prevent-related personal data. When a public authority refers a person to the Prevent process, or indeed whenever a professional makes a query regarding someone they think may require a referral, the police store the individual's personal information in a Police Case Management Tracker (PCMT). Police use PCMTs to store a range of 'biographical information' – although the types of data that may fit in this category have not been revealed publicly – as well as the nature of perceived risks or vulnerability. The police do not notify the person of their listing on the tracker,[37] while the Home Office and other government agencies can request any information contained in this database from the relevant police department.[38]

37. Other public authorities, such as immigration enforcement agencies, other police services, and education providers likely have access to information stored in the PCMT.[39] The People's Review of Prevent – an alternative review of the strategy created by individuals with lived experience of its impacts – provides a brief rundown of different databases which the researchers believe store personal data for Prevent-related purposes, alongside a list of the authorities the researchers believe are capable of accessing or requesting data from each system.[40]

38. Prevent-related data is subject to no maximum storage period in practice, and the duration of the retention can vary depending on the practitioner's assessment and the relevant professional guidance.

39. In 2020, a woman challenged the Metropolitan Police Service (MPS) for its retention of Prevent-related data about her child; specifically, she became aware that the MPS had stored data regarding a Prevent referral. The child had been referred at the age of 11, and the case was closed after six months. In 2019 – three and a half years after the initial referral – the MPS refused the mother's request to delete information regarding the referral in the MPS' database. The MPS argued that, in line with legislation and statutory guidance,[41] the court should allow it to retain the data for at least six years, further arguing that 'radicalisation is considered to be a process that occurs over time' and that 'where there is plainly a legitimate aim in retaining data for the purpose of preventing terrorist activity, we consider that retention for [this period of time]… is proportionate'[42] – despite the fact that the referring authority and the MPS recognised

---

[37] Jamie Grierson, 'Revealed: how teachers could unwittingly trigger counter-terror inquiries' (*The Guardian*, 21 February 2020).
[38] Jamie Grierson, 'Counter-terror police running secret Prevent database' (*The Guardian*, 6 October 2019).
[39] Hilary Aked, 'False Positives: the Prevent counter-extremism policy in healthcare' (*Medact*, 2020), p.60.
[40] John Holmwood and Layla Aithadj, 'The People's Review of Prevent' (February 2022), p. 106. The Metropolitan Police Service, local authorities, national counter-terrorism officers, and by other public bodies can access this data.
[41] As provided for in the police data retention guidelines: see College of Policing, 'Information management: Retention, review and disposal'.
[42] *R (on the application of II (by his mother and Litigation Friend, NK)) v. Commissioner of Police for the Metropolis* [2020] EWHC 2528 (Admin), para. 56.

that the reasons for the Prevent referral in this specific instance were untrue.[43] To note, the MPS does not publicise any Prevent-specific data protection policy.[44]

40. In analysing whether it was still proportionate to keep information about the child and the Prevent referral in a police database several years later, the High Court indicated that even when a public body has made a mistaken or unnecessary referral, personal data may still be lawfully stored after this date, if legitimate concerns about risks and other safeguarding issues persist.[45] In the circumstances of this case, however, the court concluded that it was no longer proportionate to hold the data.[46]

Data sharing agreements

41. As noted above, police services, local authorities, national counter-terrorism officers and other public bodies, including the Home Office, can access Prevent-related data through the PCMT and other databases.[47] Data sharing and storage practices appear to vary between authorities, with conflicting policies and practices implemented;[48] although some of these policies refer to human rights laws and data protection legislation, most official guidance tends to prioritise extensive data processing and sharing between authorities without seeking consent from the person concerned. In many instances, practitioners are subject to diverging policies, which may cause uncertainty about how to implement their professional obligations.

42. Outside of these databases, the Home Office, through its statutory guidance, urges specified authorities[49] – including local government authorities, schools, nurseries, NHS trusts and police chiefs – subject to the Prevent duty[50] to engage in information sharing arrangements, without reference to standards of data protection or other aspects of privacy. For instance, the Prevent duty guidance for further education institutions states:

---

[43] *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. 65-73.

[44] We recognise that the MPS likely has Prevent-specific policies; however, these are not available to the public. See Metropolitan Police Service, 'Metropolitan Police Service Appropriate Policy Document: Sensitive Processing for Law Enforcement Purposes' (updated March 2022); Metropolitan Police Service, 'Metropolitan Police Service Appropriate Policy Document: Processing Special Category and Criminal Offence Data' (March 2022).

[45] *R (on the application of II (by his mother and Litigation Friend, NK)) v. Commissioner of Police for the Metropolis* [2020] EWHC 2528 (Admin), para. 73.

[46] For various reasons, including: that the individual was a child and that almost five years had passed since the initial concern, that the referral was erroneous and the initial referrer mistaken, and that the MPS seemed to underestimate the impact of data retention on the individuals whose data had been retained: see *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. 75-79.

[47] John Holmwood and Layla Aithadj, 'The People's Review of Prevent' (February 2022), p. 106.

[48] For instance, see Jamie Grierson, 'Manchester colleges agreed to share data of students referred to counter-terror scheme' (*The Guardian*, 19 July 2020).

[49] Specified in Counter-Terrorism and Security Act 2015, Schedule 6.

[50] Found in Counter-Terrorism and Security Act 2015, s26.

'At a corporate level we would expect the [further education] institution to have robust procedures both internally and externally for sharing information about vulnerable individuals. This should include information sharing agreements where possible.'[51]

43. A few agreements created specifically for the purposes of sharing Prevent-related data are publicly available. For instance, the London School of Economics and Political Science (LSE) has published a draft data sharing agreement intended to allow the university to comply with obligations stemming from the Prevent duty – sharing data when necessary and proportionate to the aim of complying with the statutory duty.[52] While the policy emphasises consent and compliance with other statutory obligations relating to data protection and human rights, the draft agreement further authorises the sharing of people's data with authorities listed under section 37[53] and Schedule 7 of the Counter-Terrorism and Security Act 2015, which is a broad list that includes government departments, local authorities, the police, and education providers.[54]

44. The NHS likewise provides a sample data sharing agreement for use by NHS trusts (that is, units of the NHS), which is general in nature and not limited to Prevent-related data or purposes. This guidance suggests that NHS trusts should include provisions relating to patient consent and statutory approval for data sharing in these agreements, as well as requiring decision-makers to consider Article 8 of the European Convention on Human Rights (ECHR) (the right to respect for private life).[55] However, the guidance does not specifically explain how the trusts should handle Prevent-related data.

45. Besides these and other exceptions, Prevent-specific (or potentially Prevent-related) data sharing agreements are often not publicised; however, civil society organisations have made some attempts to obtain such information. In 2019, the UK human rights organisation Liberty had some – albeit limited – success in obtaining and publicising policies on data sharing and storage by public authorities under Prevent through Freedom of Information Act 2000 (FOIA) requests.[56] The organisation uncovered a 'secret' Prevent database that held a broad range of personal information, although it was unable to ascertain which bodies had access to this information, for what purposes, and how long each of the relevant authorities stored the information.[57]

46. Other attempts to increase transparency have met with less success. For example, digital rights activist Jen Persson has submitted multiple FOIA requests to child

[51] Home Office, 'Prevent duty guidance: for further education institutions in England and Wales' (*Gov.uk*, 1 April 2021), para. 22. Similar guidance exists for higher education institutions, again without reference to data protection or privacy standards: see Home Office, 'Prevent duty guidance: for higher education institutions in England and Wales' (*Gov.uk*, 1 April 2021), paras. 16-17, 23.
[52] London School of Economics and Political Science (LSE), 'Data-sharing agreement for use in compliance with Prevent statutory duty under Counter-Terrorism and Security Act 2015' (April 2018), paras. 1, 3-4.
[53] For members of Channel panels.
[54] London School of Economics and Political Science (LSE), 'Data-sharing agreement for use in compliance with Prevent statutory duty under Counter-Terrorism and Security Act 2015' (April 2018), paras. 5, 8.
[55] NHSX, 'Data sharing template' (*NHS*, 18 December 2020).
[56] Under the Freedom of Information Act 2000, s1.
[57] Liberty, 'Liberty uncovers secret Prevent database' (*Liberty*, 7 October 2019).

safeguarding boards charged with implementing the Prevent duty.[58] Persson requested:

a. Documents that the child or their parent or guardian receives before the safeguarding board shares personal information with third parties as part of the Channel programme; and

b. Data regarding the total number of onward contact points involved in information sharing as a result of a Channel panel review, including lists of involved third party organisations.

47. The safeguarding boards refused these requests, on the grounds that that the boards did not hold the information requested or that the information was exempt from disclosure on national security grounds (which the boards argued particularly regarding the recipients of shared data). Some bodies also stated that they did not have Channel-specific privacy notices at this stage (or claimed that other bodies such as the local police service instead held the requested information); however, evidence described throughout this report suggests that many local authorities do have Prevent-specific data protection policies in place – and some even publicise these. Therefore, there appears to be some inconsistency in how authorities interpret the national security exemptions under FOIA. Regardless, this lack of transparency is emblematic of the generally opaque nature of Prevent processes, particularly when it comes to the handling of people's personal data.

48. We have located an example of a local authority in England that publicises its Prevent-specific privacy policy. The Council's policy provides greater depth in comparison to other authorities' publicly available policies, and we reproduce it here at length to illustrate how decision-makers may implement competing legal and policy considerations in practice. (We discuss this policy, as written, for illustration purposes only and are not claiming that the Council has broken any laws or otherwise engaged in wrongdoing.)

49. The Council's policy states that:

'Effective information sharing is key to the delivery of Prevent, so that partners are able to take appropriately informed action. This will sometimes require the sharing of personal information between partners; this is particularly the case where sharing of information will be central to providing the best support to vulnerable individuals.

…

Partners may consider sharing personal information with each other for Prevent purposes, subject to a case by case basis assessment which considers whether the informed consent of the individual can be obtained and the proposed sharing being [sic] necessary, proportionate and lawful. [Their emphasis]

[58] The WhatDoTheyKnow platform holds the records of these FOIA requests.

…

The overriding principles are necessity and proportionality. It should be confirmed by those holding information that to conduct the work in question it is necessary to share the information they hold. Only the information required to have the desired outcome should be shared, and only to those partners necessary. Key to determining the necessity and proportionality of sharing information will be the professional judgement of the risks to an individual or the public. Consideration should also be given to whether discussion of a case is possible with anonymised information, for example, referring to "the young person" without the need to give the individual's name, address or any other information which might identify them.

…

The default should be to consider seeking the consent of the individual to share information. There will, of course, be circumstances in which seeking the consent of the individual will not be desirable or possible, because it will prejudice delivery of the intended outcome, and there may be gateways or exemptions which permit sharing to take place without consent.' [59]

50. This policy is very general rather than setting clear, specific parameters or requirements; appears to prioritise 'effective information sharing'; and provides only limited guidance on consent and individual rights. In our view, the overall thrust of the policy is toward information sharing, even if the text encourages certain protective measures such as 'anonymised information'. The recommendation to 'consider' seeking consent is also followed by a longer and more detailed discussion of possible exceptions. The legalistic but non-specific nature of the language in the policy may further render it difficult for non-lawyers to apply.

Prevent guidance and training

51. Before discussing parts of the Prevent guidance relevant to data processing, it should be noted that the UK government is reconsidering certain aspects of its guidance relating to higher education and further education institutions in light of the *R (Butt) v. Secretary of State for the Home Department*[60] judgment, which concluded that the Higher Education Funding Council's – the former statutory monitoring body for higher education institutions – guidance for higher education bodies when considering whether to book speakers – which may hold 'extremist' views – for university events, was unbalanced and tended towards limiting freedom of speech.[61] However, any action is unlikely to address the data protection issues outlined elsewhere in this report, as

[59] South Gloucestershire Council, 'Prevent – referrals and Channel process' (*South Gloucestershire Council*), Appendix 3. See also Hampshire County Council, 'PREVENT privacy notice' (*Hampshire County Council*). The policy refers to central guidance by policing adjacent bodies Association of Chief Police Officers and National Policing Improvement Agency, 'Guidance on the Management of Police Information' (2nd edn, 2010).

[60] *R (Butt) v. Secretary of State for the Home Department* [2019] EWCA Civ 256.

[61] Home Office, 'Prevent duty guidance' (*Gov.uk*, 1 April 2021). The Office for Students now holds this function.

this decision concerned the guidance on event speakers and freedom of speech and not personal data or other privacy issues.[62]

52. The Home Office's most recent statutory guidance on Prevent (updated in April 2021) provides members of authorities subject to the Prevent duty with guidance on how to fulfil this obligation to have 'due regard to the need to prevent people from being drawn into terrorism', which involves bodies working together to highlight and react to individual cases where they deem an individual is at risk, while the specified authorities must also ensure that they create training and policies for staff to follow in implementing the duty.[63] The statutory guidance states that:

'In fulfilling the duty in section 26 of the Act, we expect all specified authorities to participate fully in work to prevent people from being drawn into terrorism.'[64]

The Home Office emphasises the importance of cooperation, for instance through sharing personal data with the police, even though Prevent purportedly is not a criminal justice programme.

53. One section, titled 'A risk-based approach to the *Prevent* duty', points to a security-centric approach, as opposed to one focused on safeguarding the person affected – the ostensible purpose of Prevent, a programme that does not require any suspicion that the person might engage in violence, and indeed appears to impact many people whose activities are peaceful.[65] The Home Office also places consistent emphasis on the importance of cooperation, for instance through sharing personal data, between the specified authorities and the police, among others – even though Prevent purportedly is not a criminal justice programme.[66]

54. The statutory Prevent guidance does explain the role of data sharing as part of the policy. Within this guidance, there are multiple limitations placed on data sharing for

---

[62] The operative part of the judgment is found at *R (Butt) v. Secretary of State for the Home Department* [2019] EWCA Civ 256, paras. 158-177. For a summary, see Damien Gayle, 'UK's Prevent guidance to universities unlawful, court rules' (*The Guardian*, 8 March 2019).

[63] Issued under s29 Counter-Terrorism and Security Act 2015; Home Office, 'Revised Prevent duty guidance: for England and Wales' (*Gov.uk*, 1 April 2021), para. 4.

[64] Home Office, 'Revised Prevent duty guidance: for England and Wales' (*Gov.uk*, 1 April 2021), para. 12.

[65] Schools and other education providers, as well as healthcare providers and prisons, take a similar approach: see Home Office, 'Revised Prevent duty guidance: for England and Wales' (*Gov.uk*, 1 April 2021), paras. 67-68, 91, 106-118, 127-129. See also the same with regard to the Channel process: see HM Government, 'Channel Duty Guidance: Protecting people vulnerable to being drawn into terrorism' (2020), paras. 109-117. For more information on Prevent as a safeguarding tool, see Joel Busher and Lee Jerome (eds.), *The Prevent Duty in Education: Impact, Enactment and Implications* (Basingstoke: Palgrave Macmillan, 2020); P. Daniel Silk, Basia Spalek and Mary O'Rawe (eds.), *Preventing Ideological Violence* (Basingstoke: Palgrave Macmillan, 2013). For example, see Wiltshire Council Community Safety Team, 'The Prevent Duty – Safeguarding from radicalisation' (*Wiltshire Council*, 2022).

[66] Home Office, 'Revised Prevent duty guidance: for England and Wales' (*Gov.uk*, 1 April 2021), paras. 17, 33-37, 48, 69, 87-90, 126, 143-144.

Prevent purposes – with these obligations placed on public authorities rather than individual practitioners – including:[67]

a. Information sharing is generally governed by legislation, and legislation must exist to grant such powers to the authority;

b. Principles of necessity and proportionality are central to determining whether to share data about people; and

c. The authority should obtain consent from the individual 'wherever possible' prior to sharing the data.

Prevent guidance dedicates much more space to monitoring and enforcement than it does to ensuring lawful, voluntary and consensual referrals.

55. These limitations on the rights of the referred individual are only mentioned in two paragraphs of the guidance, which otherwise focuses predominantly on security risks a government agency believes the person may pose (a belief that does not need to be based on evidence) and the necessity of a referral, while also lengthily explaining the Home Office's monitoring and enforcement powers over authorities which fail to comply with their legal duty to report people.[68] The guidance dedicates much more space to monitoring and enforcement than it does to ensuring lawful, voluntary and consensual referrals.[69]

56. Many government departments have issued similar guidance for their specific industries. For instance, the DfE has issued statutory guidance for education providers,[70] which tends towards the sharing of data on the basis of the best interests of the child, without necessarily seeking the child's (or their parent's or guardian's) consent. For instance, in the context of general data sharing:

'…DPA and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe and promoting their welfare. If in any doubt about sharing information, staff should speak to the designated safeguarding lead or a deputy. Fears

[67] Home Office, 'Revised Prevent duty guidance: for England and Wales' (*Gov.uk*, 1 April 2021), paras. 21-22.
[68] Also see Home Office, 'Prevent duty guidance: for further education institutions in England and Wales' (*Gov.uk*, 1 April 2021), paras. 3, 6, 9-11, 14-18.
[69] Home Office, 'Revised Prevent duty guidance: for England and Wales' (*Gov.uk*, 1 April 2021), paras. 23-28, 52-56, 72-76, 96-98, 132-136, 145; Home Office, 'Prevent duty guidance: for further education institutions in England and Wales' (*Gov.uk*, 1 April 2021), paras. 29-31; Home Office, 'Prevent duty guidance: for higher education institutions in England and Wales' (*Gov.uk*, 1 April 2021), para. 31.
[70] To the contrary there is separate departmental guidance from the Department for Education on the Prevent duty, which instead advises staff members to follow the usual safeguarding processes and involve family decision-making as best practice: see Department for Education, 'The Prevent duty: Departmental advice for schools and childcare providers' (2015), pp. 7, 10.

*about sharing information **must not** be allowed to stand in the way of the need to safeguard and promote the welfare of children.'*[71] *[Their emphasis]*

57. NHS England takes a somewhat different approach to data sharing, instead couching its guidance on the basis of legal guidelines, including data protection principles and human rights legislation. In summary, the NHS takes a much more balanced approach than that seen in other guidelines regarding data sharing.[72] However, it appears that the NHS has altered its guidance in response to concerns health care practitioners have raised that they be required to over-share personal information for the purposes of Prevent:

    'The guidance has been developed in response to concerns raised by health care practitioners about information sharing for the purposes of Prevent and Channel particularly when:

    - *They are requested to share information without the individuals' prior consent or*
    - *The individual has not been explicitly identified as being at risk of harm, abuse or exploitation.'* [73]

Questions Ofsted asked education providers paid no apparent attention to whether human rights and data protection standards were upheld.

58. Ofsted, the non-ministerial government department responsible for monitoring the implementation of the Prevent duty in higher education, released a report in 2021 on how further education institutions have satisfied the Prevent duty. The questions the department asked education providers in monitoring their compliance with the duty turned towards reviewing the efficacy of Prevent, with no apparent attention paid to whether human rights and data protection standards were upheld (the report did not mention these concepts at all, and neither have other Prevent monitoring reports).[74] The Ofsted report was also highly critical of current data sharing agreements related to Prevent, arguing that these should be *more* expansive than those currently in force.[75] The questions addressed were:

---

[71] HM Government, 'Keeping children safe in education 2021: Statutory guidance for schools and colleges' (September 2021), para. 60. Similar statements are also repeated at para. 110. See also, HM Government, 'Working Together to Safeguard Children: A guide to inter-agency working to safeguard and promote the welfare of children', paras. 27-28.
[72] See also NHS England, 'Safeguarding Adults' (February 2017), pp. 22-27.
[73] NHS England, 'Practical Guidance on the sharing of information and information governance for all NHS organisations specifically for Prevent and the Channel process' (July 2017), para. 1.3.
[74] For instance, see Office for Students, 'Prevent monitoring: Summary of annual accountability and data returns: 2017-18, 2018-19, 2019-20' (2 September 2021).
[75] Ofsted, 'How well are further education and skills providers implementing the 'Prevent' duty?' (July 2016), pp. 4-8.

- *'Are providers ensuring that external speakers and events are appropriately risk assessed to safeguard learners?*
- *Are the partnerships between different agencies effective in identifying and reducing the spread of extremist influences?*
- *Are providers assessing the risks that their learners may face, and taking effective action to reduce these risks?*
- *Are learners being protected from inappropriate use of the internet and social media?*
- *To what extent are staff training and pastoral welfare support contributing to learners' safety?'* [76]

59. Similarly, the General Medical Council (GMC), the independent regulator for doctors in the UK, does not have specific Prevent guidance for its members; however it has drafted one on confidentiality, which is applicable to data sharing under Prevent.[77] Although this guidance appears to give weight to the data protection principles outlined below, the GMC advises that its members need not seek consent to use personal data for purposes other than the initial treatment if 'the information is required by law, or it is not appropriate or applicable to obtain consent'.[78] Under this guidance, the practitioner may exclude the patient from the decision to use or share Prevent-related personal data.

60. By contrast, the British Medical Association – the representative organisation for doctors and medical students – advises that practitioners cannot use Prevent alone as a ground for sharing personal information.[79]

61. Therefore, in the medical field, at least, there appears to be divergence in advice, and presumably in practice.

4. Missing information regarding data processing under Prevent

62. Presently, there is a general lack of publicly available information on the policies and practices of specific public bodies. Although government guidance exists and provides some evidence as to how public authorities treat personal data for the purposes of Prevent, such guidance is of limited utility in assessing the legality of the practice, as each body has discretion in how to act, and the above factual outline indicates at least some divergence in practice between public bodies.

---

[76] Ofsted, 'How well are further education and skills providers implementing the 'Prevent' duty?' (July 2016), p. 3.
[77] General Medical Council, 'Confidentiality: good practice in handling patient information'. The General Medical Council has statutory authority to register and licence medical professionals, as well as to advise on best practices and medical ethics: see Medical Act 1983.
[78] General Medical Council, 'Confidentiality: good practice in handling patient information', para. 95.
[79] British Medical Association, 'Adult safeguarding – a toolkit' (2018), pp. 46-48.

The European Convention on Human Rights requires that government interferences with private life must be authorised by clear, specific, accessible laws – not secret policies.

63. The fact that crucial information is missing violates human rights, as discussed below. Article 8 of the ECHR requires that government interferences with private life must be authorised by clear, specific, accessible laws – not secret policies.

64. Beyond this, in order to assess fully the legality of Prevent-related data collection and processing by any particular body in the UK, we would need the following further information:

    a. Information about how the body ensures compliance for data protection and human rights laws when it gathers, stores, shares, accesses and otherwise handles personal data:
        i. How does the body collect Prevent-related data? Does the body receive the data from a third party, such as when police receive data from schools?
        ii. Why does the body gather or use Prevent-related personal data?
        iii. How, and for how long, does the body store Prevent-related personal data?
        iv. How does the body determine whether to retain Prevent-related personal data? Is the retention reviewed systematically?
        v. In what circumstances is Prevent-related personal data shared? To whom is the information shared and on what legal grounds?
        vi. What procedures are in place to ensure accountability for any unnecessary or otherwise unlawful use of Prevent-related personal data? How do these procedures operate if the individual is not aware that their data is being processed?
    b. Information about whether the body treats Prevent-related personal data and other personal data differently, and if so, how and why; and
    c. Information about staff training on the Prevent duty, and whether the training references the applicable human rights and data protection standards.

65. While this information would be the minimum required to engage in a full legal analysis of the legality of current Prevent-related data processing, we can draw some preliminary conclusions regarding the legality of Prevent-related data practices based on what we know.

5. Legal framework on data processing in the context of Prevent

66. Here, we provide a summary of some of the privacy laws that apply to data collected, stored and shared under Prevent. Understanding these laws allows us to assess whether Prevent-related practices are breaking them.

Data protection legislation

67. The Data Protection Act 2018 (DPA) and the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 regulate data protection in the UK (referred to as the UK GDPR), augmenting the General Data Protection Regulation (GDPR).[80] Despite being a European Union (EU) legal instrument, similar provisions to those in the GDPR still apply in the UK following the country's withdrawal from that institution.[81]

68. There are three main pillars of the data protection regime in the UK: the fair processing of data on a lawful basis; the right of an individual to obtain information about the processing of their personal data; and a range of monitoring and enforcement powers. Organisations – not just public authorities – processing Prevent-related data must adhere to seven data protection norms: lawfulness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability.[82]

69. However, special regulations apply to law-enforcement-related data use and to the intelligence services, namely the Security Service, the Secret Intelligence Service and the Government Communications Headquarters (GCHQ).[83] For instance, if a local council has referred an individual to Prevent, and subsequently shared this information with the intelligence services, then the same information could be subject to a different legal framework. Each of the principles may apply differently to data processing by these bodies and for these purposes.

70. The lawfulness and transparency obligation requires a valid legal ground for collecting and processing personal data, only fair and expected uses of the data, and an openness about the processing and collection of the data.[84]

71. The UK GDPR provides many potential grounds for collecting and using personal data. When school personnel, for example, believe they may need to make a Prevent referral, the school will have to satisfy itself that there is a lawful ground for processing the individual's personal data. For instance, Section 8 of the DPA provides a basis for lawful

---

[80] Data Protection Act 2018, s1(2)-(3); Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019, SI 419/2019; General Data Protection Regulation.

[81] Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019, SI 419/2019, regulations 2 and 5; European Union (Withdrawal) Act 2018, s3. The UK courts have concluded that some DPA provisions are incompatible with the GDPR, and are therefore unlawful: for instance, see *R (on the application of The Open Rights Group and another) v. Secretary of State for the Home Department and another* [2021] EWCA Civ 800.

[82] General Data Protection Regulation, Article 5.

[83] Data Protection Act 2018, Part 3 (law enforcement processing), Part 4 (intelligence service processing) and Schedule 8 (processing conditions for law enforcement). See also s82(2) for the list of intelligence services subject to the obligations outlined in Part 4.

[84] The principle is sometimes termed 'lawfulness, fairness, and transparency'. For the definition of 'personal data', see Data Protection Act 2018, s3; *NHS Business Services Authority v. Information Commissioner* [2021] UKUT 192 (AAC). Data Protection Act 2018, s35(1) (for 'law enforcement purposes') and s86 (when by the intelligence services). See, generally, Data Protection Act 2018, s2(1)(a); Information Commissioner's Office, 'Principle (a): Lawfulness, fairness and transparency' (*ICO*); *YZ v. Chief Constable of South Wales Police* [2022] EWCA Civ 683, paras. 26-29, 50-55, 63-69; *Hussain v. Sandwell Metropolitan Borough Council* [2017] EWHC 1641 (Admin), paras. 229-237; *Johnson v. Medical Defence Union* [2007] EWCA Civ 262.

processing of data when this is necessary in the public interest: section 8(c) provides an exemption to usual restrictions based on 'the exercise of a function conferred on a person by an enactment or rule of law'.[85]

72. One notable omission from this list of principles is consent, as it is not an absolute requirement when processing people's data if there is some other legal basis for the processing. Those participating in Prevent – including the referring party, members of the Channel panel, or organisations which receive Prevent-related data – can, therefore, share and retain personal data of the referred person without that person's consent if they can satisfy one or more of the other grounds for lawful processing. In other words, people can consent to having their data collected and otherwise processed, but if they do not, authorities may still be able to do so on certain other limited grounds.

73. The purpose limitation principle has three main aspects: first, the data processor must inform the data subject (that is, the person the information concerns) of the purpose of the data collection and processing *before* that collection or processing happens. Second, the processor must record this original purpose, and the processor may only use the personal data for this original purpose.[86] If the processor wishes to use the collected information for another purpose, they can only do so if these new purposes are compatible with the original purpose, if the data subject has consented to data processing for this new purpose, or if there is a legal ground for processing without consent. For example, if a local police force receives information under Prevent, but then uses that information for law enforcement purposes, then the police force would need to satisfy itself that it had another legal ground for using the data for this new purpose.

74. Data minimisation requires that data controllers collect only relevant data, while limiting the amount of data collected to that which is necessary to fulfil the stated purpose.[87]

75. To ensure that data collection and other processing meet the accuracy requirement, controllers must ensure that the data processed is correct and not misleading. This is a continuous obligation, and does not apply solely when the data controller first collects the information.[88] In some instances, data controllers are under obligations to ensure that they update the personal data they hold; in the Prevent context, this might – for example – require the controller to mark an expired referral as 'historical', or note whether the referral was erroneous. When the

---

[85] *R (on the application of HM) v. Secretary of State for the Home Department* [2022] EWHC 695 (Admin), paras. 34-35. See also, General Data Protection Regulation, Article 6(e).

[86] Data Protection Act 2018, s36(1) (for 'law enforcement purposes') and s87 (when by the intelligence services). See, generally, Information Commissioner's Office, 'Principle (b): Purpose limitation' (*ICO*); *CLG and others v. Chief Constable of Merseyside Police* [2014] EWHC 60 (QB), paras. 41-46.

[87] Data Protection Act 2018, s37(1) (for 'law enforcement purposes') and s88 (when by the intelligence services). See, generally, Information Commissioner's Office, 'Principle (c): Data minimisation' (*ICO*); *Hussain v. Sandwell Metropolitan Borough Council* [2017] EWHC 1641 (Admin), para. 238; *CLG and others v. Chief Constable of Merseyside Police* [2014] EWHC 60 (QB), paras. 41-46.

[88] Data Protection Act 2018, s38(1) (for 'law enforcement purposes') and s89 (when by the intelligence services). See, generally, Information Commissioner's Office, 'Principle (d): Accuracy' (*ICO*); *Hussain v. Sandwell Metropolitan Borough Council* [2017] EWHC 1641 (Admin), para. 238; *Jackson v. Hampshire Hospitals NHS Foundation Trust* [2014] EWHC 3954 (QB), paras. 26-30.

processor continues to process information, they must update it.

76. The storage limitation obligation means that processors can only hold personal data for as long as necessary to meet the relevant purpose.[89] There is no universal time limit placed on the storage of data; however, there must be a periodic review of the necessity of continued storage. Additionally, data controllers must ensure that organisational and technical measures are in place so that data is not stored for longer than is necessary. Guidance from the Information Commissioner's Office (ICO) states that indefinite storage of personal data is generally unlawful, with three exceptions: archiving in the public interest, scientific or historical research, and statistical research.[90]

77. To ensure that these principles are effectively implemented in practice, the accountability principle mandates that data processors should be able to demonstrate their compliance with data protection legislation.[91] For example, an NHS trust must have appropriate policies, procedures and records in place to demonstrate that it can – and does – comply with its data protection obligations.

78. Alongside these obligations, data protection legislation affords greater protection to certain types of personal data, to ensure that data processors use more sensitive personal information with greater caution. This applies to information which:

    'reveal[s] racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.'[92]

79. To process this information even though it is sensitive, the processor must satisfy one of several conditions; the relevant condition for Prevent purposes is the existence of a 'substantial public interest'.[93] Processors can rely on this condition in many circumstances. For example, in the Prevent context, a public authority may argue that they are processing an individual's data for statutory or government functions, or to safeguard children or individuals at risk.[94]

80. However, the DPA also contains a broad overarching 'national security and defence' exemption to many of the norms and principles outlined elsewhere in the DPA and in the UK GDPR. This means that many of the data protection requirements under domestic law do not apply when a public body uses data for national security or defence purposes, even when this data would otherwise require additional degrees of

[89] Data Protection Act 2018, s39 (for 'law enforcement purposes') and s90 (when by the intelligence services). See, generally, Information Commissioner's Office, 'Principle (e): Storage limitation' (*ICO*).
[90] Information Commissioner's Office, 'Principle (e): Storage limitation' (*ICO*).
[91] Information Commissioner's Office, 'Accountability and governance' (*ICO*).
[92] General Data Protection Regulation, Article 9(1).
[93] Data Protection Act 2018, s10(1)(b); General Data Protection Regulation, Article 2(g).
[94] Data Protection Act 2018, Schedule 1, paras. 6 and 18 respectively. On data protection and safeguarding in the law enforcement context, see *R (on the application of M) v. Chief Constable of Sussex Police* [2021] EWCA Civ 42.

protection.[95] However, the body must nonetheless hold a legal ground for processing the data.[96] Additionally, the ECHR right to respect for private life (discussed below), which covers many aspects of data protection, does not include a wholesale national security or defence exception. Outside of these caveats, the UK courts have applied the exception expansively, taking the view that the government should be able to process data that is necessary for national security purposes, while giving individual rights less priority in decision-making.[97]

81. Of particular relevance to the Prevent context is the law applicable to the intelligence services (as explained below, there are separate provisions for law enforcement data processing under the DPA, but these are not applicable to Prevent-related data processing). To be lawful, handling of personal data by the intelligence services must meet one of the conditions listed in Schedule 9 to the DPA, and, if processing sensitive data, the body must also use one of the conditions in Schedule 10.[98] Schedule 9 allows data processing necessary to comply with a legal obligation, to protect the 'vital interests' of the individual or another person, to comply with a 'function[] conferred … by an enactment or rule of law' or in the exercise of government functions or in the public interest, or to pursue the legitimate interests of the controller or to relevant third parties.[99] Schedule 10 conditions are similar to those included in Schedule 9, except for the removal of the 'public interest' and 'legitimate interests' grounds.[100]

82. These data processing grounds are broad and could allow the receipt and handling of Prevent data by the intelligence agencies, potentially on a massive scale.

European Convention on Human Rights

The UK must follow the European Convention on Human Rights, and not only its own laws, when authorities process and store personal information.

83. The UK must follow the European Convention on Human Rights, and not only its own laws, when authorities process and store personal information. Although a range of human rights treaties that the UK has ratified, or otherwise supported, are potentially relevant to this area of the law,[101] this legal briefing will pay particularly close attention

[95] Which must also satisfy the requirements of Data Protection Act 2018, s7. s26(2) and s28(1) outline the norms for such bodies to follow when processing personal data for national security or defence purposes. See also s79 on the role of government ministers in designating certain matters as 'national security' concerns. On 'national security' under the DPA generally, see *Williams v. Information Commissioner and Chief Constable of Kent Police* [2021] UTAAC 149 (AAC).
[96] Data Protection Act 2018, s26(2)(a); for international transfers relevant to national security and criminal prosecution, see *R (on the application of Elgizouli) v. Secretary of State for the Home Department* [2020] EWHC 2516 (Admin).
[97] See *QX v. Secretary of State for the Home Department* [2020] EWHC 1221 (Admin), paras. 90-91.
[98] Data Protection Act 2018, s86(2).
[99] Data Protection Act 2018, Schedule 9, paras. 3, 4, 5(c-e) and 6 respectively.
[100] Data Protection Act 2018, Schedule 10, paras. 3, 4 and 7(b-d).
[101] E.g., International Covenant on Civil and Political Rights, New York, 16 December 1966, entered into force 23 March 1976, 999 UNTS 171, Article 17; Convention on the Rights of the Child, New York, 20 November 1989, entered into force 2 September 1990, 1577 UNTS 3, Article 16; Convention on the Rights of Persons with Disabilities, New York, 13 December 2006, entered into force 3 May 2008, 2515

to the ECHR, which the Human Rights Act 1998 (HRA) gives domestic effect in UK law – that is, people can bring claims in UK courts for violations of their human rights under the ECHR, and judges can order that the government stop doing something, pay damages or take other measures.[102]

84. Article 8 of the ECHR guarantees respect for the right to private and family life, establishing that:

'1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'

Interference

85. A person who wants to challenge the processing of their personal data by a public authority under Prevent, based on their human rights under Article 8 of the ECHR, must first demonstrate that there has been an interference with their private life. The concept of 'private life' can include various aspects of a person's identity, including – for example – their name, photo and biometric information.[103] The European Court of Human Rights (ECtHR) has stated that the concept of 'private life' cannot be defined exhaustively; in other words, it can evolve and expand over time, and the ECtHR has extended its meaning many times to include various aspects of a person's identity, such as their gender identity and sexual orientation.[104] In other words, what counts as 'private life' is a question the Court is constantly revisiting, especially as technology evolves and urgent new issues arise.

UNTS 3, Article 22; Convention for the protection of individuals with regard to automatic processing of personal data, Strasbourg, 28 January 1981, entered into force 1 October 1985, 1496 UNTS 65. There is additionally a broad range of guidance prepared by international actors, most notably the UN High Commissioner for Human Rights, the European Data Protection Board, and the Organisation for Economic Co-operation and Development: see United Nations High Commissioner for Human Rights, 'The right to privacy in the digital age', Human Rights Council, Forty-eighth session, 13 September 2021, A/HRC/48/31; European Data Protection Board, 'Endorsed WP29 Guidelines' (2016); Organisation for Economic Co-operation and Development, 'Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data', OECD/LEGAL/0188, 11 July 2013. For an overview, see Privacy International, 'Guide to International Law and Surveillance 2.0' (February 2019); Kristian P. Humble, 'International law, surveillance and the protection of privacy' (2021) 25(1) International Journal of Human Rights 1.

[102] Human Rights Act 1998, s1.

[103] App. Nos. 47621/13, 3867/14, 73094/14, 19298/15, 19306/15 and 43883/15, *Vavřička and others v. the Czech Republic*, Judgment, 8 April 2021, para. 261.

[104] App. No. 13710/88, *Niemietz v. Germany*, Judgment, 16 December 1992, para. 29. The jurisprudence suggests that the main matter for domestic courts to consider is whether the individual can legitimately expect the authority not to share or publish the information without their consent: see App. No. 39954/08, *Axel Springer AG v. Germany*, Judgment, 7 February 2012, para. 83; App. No. 36345/16, *L.B. v. Hungary*, Judgment, 12 January 2021, paras. 21-22.

Historically, the Court has demonstrated a great awareness of how governments can misuse personal information for repression.

86. Historically, the Court has demonstrated a great awareness of how governments can misuse personal information for repression, and therefore has interpreted the Article 8 right expansively. The ECHR was created in the wake of the Second World War, when mass collections of personal information contributed to deportations and other deadly persecution of Jewish people.[105] What is now the ECtHR began deciding cases at a time when governments such as East Germany's were suspected of creating dossiers about people's private lives and targeting dissidents.[106] Some of the Court's most important cases concerning Article 8 to date have involved, for example, secret legislation allowing Russian security services to systemically collect telephone communications data from service providers, extensive secret surveillance powers in post-War Germany, indefinite storage of DNA profiles, and the inability to challenge the accuracy of data the state holds about an individual.[107]

87. Today, 'private life' under the ECHR can include information that a person may openly share in public – such as information about a person's public location obtained through records of ticket purchases for public transport.[108] Therefore, if a person publicises their religious beliefs, political views, sexual orientation or mental health matters on social media, for example, their right to privacy is not necessarily affected. The government cannot necessarily gather and store this kind of information just because the person has previously shared it with others.

88. The UK courts have continued to grapple with this question of the extent to which information that is not strictly secret may still be 'private' under human rights law, including in the *Butt* case. In *Butt*, the applicant challenged the Home Office's (and other public bodies') processing of their personal data under Prevent; the Court of Appeal for England and Wales concluded that the collection and retention of information about Butt's religious views was lawful on the basis that these were already public knowledge, and that the claimant therefore did not have any reasonable expectation of privacy (which, according to the Court of Appeal, meant that Article 8 of the ECHR was not engaged). In any case, the Court concluded that any interference

---

[105] For an overview, see Thomas Shaw, 'Privacy Law and History: WWII-Forward' (*IAPP*, 1 March 2013).
[106] For instance, see Christiane Olive, *Creating a Democratic Civil Society in Eastern Germany: The Case of the Citizen Movements and Alliance* (Basingstoke: Palgrave Macmillan, 2001); Katrina Gulliver, 'The opt-out illusion: How we have acquiesced to losing our privacy' (*Times Literary Supplement*, 12 April 2019).
[107] See App. No. 47143/06, *Zakharov v. Russia*, Judgment, 4 December 2015; App. No. 5029/71, *Klass and others v. Germany*, Judgment, 6 September 1978, App. Nos. 53205/13 and 63320/13, *Trajkovski and Chipovski v. North Macedonia*, Judgment, 13 February 2020 and App. No. 28341/95, *Rotaru v. Romania*, Judgment, 4 May 2000 respectively.
[108] App. Nos. 40660/08, 60641/08, *Von Hannover v. Germany (No. 2)*, Judgment, 7 February 2012, para. 95. In Application No. 30194/09, *Shimovolos v. Russia*, Judgment, 21 June 2011, the ECtHR held that such information was within the applicants 'zone of interaction… with others' (see also: App. No. 63737/00, *Perry v. the United Kingdom*, Judgment, 17 July 2003, para. 36; App. No. 44647/98, *Peck v. the United Kingdom*, Judgment, 28 January 2003, para. 57; App. No. 44787.98, *P.G. and J.H v. the United Kingdom*, Judgment, 25 September 2001, para. 56), and therefore the data was protected by Article 8 (at paras. 64-66).

would have been lawful under Article 8(2), as the restriction was a necessary and proportionate one, and done in pursuance of a legitimate aim.[109] However, the case has not reached the ECtHR and should not necessarily be taken as an indication of how the European Court would rule.

The Court recognises that privacy and secrecy are not the same thing: information can still be protected by privacy rights even if a person does not keep that information secret from all other people.

89. To the contrary, the ECtHR has held that whether an individual has a 'reasonable expectation of privacy' is not necessarily conclusive in determining whether there has been an interference with private life; indeed, 'reasonable expectation of privacy' is not a standard the Court historically has used.[110] As data protection is an inherently important aspect of Article 8, the Court ensures that even when information is in the public domain, the individual can still hold human rights protections under the ECHR when processors use the data in a manner or to a degree that the person would not have foreseen.[111] The Court recognises that privacy and secrecy are not the same thing: information can still be protected by privacy rights even if a person does not keep that information secret from all other people.[112]

90. Given the intrusive and broad nature of possible data processing under Prevent, one could question whether the UK Court of Appeal's judgment in *Butt* failed to give enough weight to the human rights standards. In other words, it is possible that under the ECHR, *Butt* was wrongly decided.

91. The ECtHR has – similarly to the UK GDPR – established that certain categories of personal data are 'sensitive' and therefore require heightened protection.[113] These include information regarding an individual's racial or ethnic origin,[114] political

[109] See *R (Butt) v. Secretary of State for the Home Department* [2019] EWCA Civ 256, paras. 53-145. There is a similar approach under UK data protection legislation: see Data Protection Act 2018, s32 and Schedule 8, para. 5.
[110] App. No. 62357/14, *Benedik v. Slovenia*, Judgment, 24 April 2018, para. 101. Albeit, the UK courts appear to have attached particular weight to this factor: see *R (Butt) v. Secretary of State for the Home Department* [2019] EWCA Civ 256, paras. 55-66; *R (Catt) v. Association of Chief Police Officers of England, Wales and Northern Ireland* [2015] UKSC 9, paras. 5-6; *Re JR38* [2015] UKSC 42, paras. 84-87, 98, 105-109; *R (W) v. Secretary of State for Health* [2015] EWCA Civ 1034.
[111] App. No. 931/13, *Oy and Oy v. Finland*, Judgment, 27 June 2017, paras. 133-138.
[112] For the conceptual distinction, see Carol Warren and Barbara Laslett, 'Privacy and Secrecy: A Conceptual Comparison' (1977) 33(3) Journal of Social Issues 43; Christine S. Scott-Hayward, Henry F. Fradella and Ryan G. Fischer, 'Does Privacy Require Secrecy? Societal Expectations of Privacy in the Digital Age' (2015-2016) 43 American Journal of Criminal Law 19.
[113] See Council of Europe, 'Guide to the Case-Law of the European Court of Human Rights: Data protection' (30 April 2021), paras. 19-37.
[114] App. Nos. 30562/04 and 30566/04, *S and Marper v. the United Kingdom*, Judgment, 4 December 2008, paras. 66, 71.

opinions,[115] religious[116] and other beliefs,[117] trade union membership,[118] genetic data,[119] biometric data,[120] health,[121] sex life[122] and sexual orientation, criminal offences, and convictions.[123] Since the ECtHR decides these issues on a case-by-case basis, it may someday decide that other types of personal data are also especially sensitive.

92. Although whether the handling of personal data respects human rights under the ECHR is something judges and scholars usually analyse under Article 8, other parts of the human rights treaty are also relevant and could provide protections. For example, the rights to freedom of expression; freedom of thought, conscience and religion; and freedom of association use similar standards. For example, a public body could violate Article 9, the freedom of religion, if it forces an individual to disclose their religious beliefs.[124]

The mere storing of information can amount to an interference with private life under the expansive protection afforded by the Convention.

93. The mere storing of information can amount to an interference with private life under the expansive protection afforded by the Article 8 right.[125] In sum, whether storing or sharing of information amounts to an 'interference' with the right to privacy will depend on the situation as well as the content of the data collected.[126]

94. Of further relevance to Prevent, the *en masse* and systematic collection and storage of data can amount to an interference in private life.[127] The mere existence of a law allowing data collection without requiring the government to disclose its collection, sharing or storage practices can amount to an interference with the Article 8 right to privacy, the Court has found in the context of large-scale surveillance of

[115] App. No. 43514/15, *Catt v. the United Kingdom*, Judgment, 24 January 2019, para. 112
[116] App. No. 21924/05, *Işik v. Turkey*, Judgment, 2 February 2010, para. 37.
[117] App. No. 66490/09, *Mockutė v. Lithuania*, Judgment, 27 February 2018, para. 117; App. No. 21924/05, *Işik v. Turkey*, Judgment, 2 February 2010, para. 37.
[118] App. No. 43514/15, *Catt v. the United Kingdom*, Judgment, 24 January 2019, paras. 112, 117-119, 123.
[119] App. No. 41079/16, *Caruana v. Malta*, Decision, 15 May 2018; App. Nos. 53205/13 and 63320/13, *Trajkovski and Chipovski v. North Macedonia*, Judgment, 13 February 2020; App. No. 62257/15, *Mifsud v. Malta*, Judgment, 29 January 2019; App. No. 8806/12, *Aycaguer v. France*, Judgment, 22 June 2017.
[120] App. Nos. 8022/77, 8025/77 and 8027/77, *McVeigh and others v. the United Kingdom*, Judgment, 18 March 1981; App. No. 18291/91, *Kinnunen v. Finland*, Admissibility (Commission), 13 October 1993; App. No. 11379/03, *Dimitrov-Kazakov v. Bulgaria*, Judgment, 10 February 2011; App. No. 74440/17, *P.N. v. Germany*, Judgment, 11 June 2020.
[121] App. No. 42788/06, *Surikov v. Ukraine*, Judgment, 26 January 2017.
[122] App. No. 22009/93, *Z v. Finland*, Judgment, 25 February 1997, paras. 95-96, 113-114.
[123] App. No. 21010/10, *Brunet v. France*, Judgment, 18 September 2014, para. 58.
[124] App. No. 15472/02, Folgerø and others v. Norway, Judgment, 29 June 2007, para. 98.
[125] App. Nos. 30562/04 and 30566/04, *S and Marper v. the United Kingdom*, Judgment, 4 December 2008, para. 67; App. No. 62332/00, *Segerstedt-Wiberg and others v. Sweden*, Judgment, 6 June 2006, para. 73; App. Nos. 58170/13, 62322/14 and 24960/15, *Big Brother Watch and others v. the United Kingdom*, Judgment, 25 May 2021, paras. 324-331.
[126] App. Nos. 30562/04 and 30566/04, *S and Marper v. the United Kingdom*, Judgment, 4 December 2008, para. 67.
[127] App. No. 28341/95, *Rotaru v. Romania*, Judgment, 4 May 2000, para. 44.

communications.[128] In such circumstances, it can violate human rights for the government even to have such expansive powers, regardless of whether a person can prove that their own data was stored or shared (provided that they are in a category of people who could have been affected).[129] We will discuss further the impact of the secrecy of Prevent data processing policies and practices and the associated legal challenges in further detail below.

In accordance with the law

95. An interference with the right to private life under Article 8 will only be compliant with human rights under the ECHR if it also meets three other crucial conditions: the interference must be legal (in the sense of not breaking domestic or international law), pursue a legitimate aim, and be necessary to achieving that aim.

96. Under the 'legality' prong of this test, there must be a domestic law authorising the interference – and that law must be clear and accessible, with foreseeable consequences, so that people understand what the government can do, under what circumstances, and what the limits are.[130]

97. The law must also contain sufficient safeguards to ensure that policy- and decision-makers adequately consider the individual's Article 8 rights when deciding whether to share or retain data.[131]

Fulfilling a legitimate aim

98. A state can potentially interfere with the Article 8 right, without violating the ECHR, on the basis of: national security, public safety, economic well-being of the state, prevention of crime or disorder, protection of health or morals, or for the protection of rights and freedoms of others.[132] The Court has the power to decide whether an interference with privacy (or a power to engage in an interference) has a legitimate aim, although it tends to be deferential to states regarding this question – an approach

[128] App. Nos. 10439/83, 10440/83, 10441/83, 10452/83, 10512/83, 10513/83, *Mersch and others v. Luxembourg*, Commission Decision (Admissibility), 10 May 1985. On the flexibility of such admissibility requirements, see App. No. 47848/08, *Centre for Legal Resources on behalf of Câmpeanu v. Romania*, Judgment, 17 July 2014, para. 96. For a concise overview as to the admissibility of challenges to secret data collection, sharing and storage, see App. No. 47143/06, *Zakharov v. Russia*, Judgment, 4 December 2015, paras. 170-179, discussed in further detail below.

[129] App. No. 58243/00, *Liberty, British Irish Rights Watch and Irish Council for Civil Liberties v. the United Kingdom*, Judgment, 1 July 2008, paras. 56-57.

[130] App. Nos. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7136/76, *Silver v. the United Kingdom*, Judgment, 25 March 1983, para. 87; App. Nos. 58170/13, 62322/14 and 24960/15, *Big Brother Watch and others v. the United Kingdom*, Judgment, 25 May 2021, paras. 332-334; App. No. 459/18, *Saber v. Norway*, Judgment, 17 December, 2020, para. 51; App. No. 73357/14, *Falzarano v. Italy*, Decision, 15 June 2021, paras. 27-29; App. No. 30194/09, *Shimolovs v. Russia*, Judgment, 21 June 2011, para. 68; App. No. 20071/07, *Piechowicz v. Poland*, Judgment, 17 April 2012, para. 212.

[131] App. No. 4378/02, *Bykov v. Russia*, Judgment, 10 March 2009, para. 81; App. No. 59648/13, *Vig v. Hungary*, Judgment, 14 January 2021, paras. 51-62.

[132] The Court provides no definition of what a 'legitimate aim' is, but broadly speaking these are the grounds in which a member state may use to justify restricting the fundamental rights listed in the Convention and its Protocols. Not all rights can be lawfully restricted, and governments may derogate from the rights that can by relying on different justifications.

known as the 'margin of appreciation'.[133] This deference has been especially strong when the state claims its legitimate aim involves national security.[134]

Necessity

99. The Court will determine not only whether an interference had a legitimate aim, but whether it was necessary to achieving that aim. In practice, on nationally sensitive issues regarding which there is no European 'consensus' on the correct and lawful approach to take, the Court may be deferential to the state.[135] However, it always reviews these questions itself, based on the evidence before it and its understanding of what the human rights found in Article 8 require. In other words, while the Court may accept some 'margin of appreciation' in the sense of leaving governments room to make certain decisions, human rights standards are always in effect and the Court applies these standards.

100. A court applying the Article 8 right must consider whether the measures taken were necessary to achieving the legitimate aim pursued.[136] Commentators and UK courts sometimes express this requirement as 'proportionality', a term the ECtHR also sometimes uses, but the treaty standard and the one the ECtHR most commonly uses is 'necessity' or 'strict necessity'.[137] In relation to data storage, multiple case examples illustrate the ECtHR's approach to necessity.[138] In *Gaughran v. the United Kingdom*, the ECtHR ruled that the indefinite retention of custody photographs on a police database was unlawful;[139] whereas a five-year retention of a photograph of a repeat offender was, in another case, deemed proportionate due to the likelihood of reoffending, as was the taking and storing of photographs of a suspected terrorist offender without their consent.[140]

---

[133] App. No. 5493/72, *Handyside v. the United Kingdom*, Judgment, 7 December 1976, paras. 48-50. For an overview, see Yutaka Arai, 'The Margin of Appreciation Doctrine in the Jurisprudence of Article 8 of the European Convention on Human Rights' (1998) 16(1) Netherlands Quarterly of Human Rights 61; Onder Bakircioglu, 'The Application of the Margin of Appreciation Doctrine in Freedom of Expression and Public Morality Cases' (2007) 8(7) German Law Journal 711.

[134] App. No. 1537/08, *Kaushal and others v. Bulgaria*, Judgment, 2 September 2010, para. 28. Contrast with App. No. 1365/07, *C.G. and others v. Bulgaria*, Judgment, 24 April 2008, para. 43.

[135] App. No. 25358/12, *Paradiso and Campanelli v. Italy*, Judgment, 24 January 2017, para. 184.

[136] App. No. 22009/93, *Z v. Finland*, Judgment, 25 February 1997, para. 94.

[137] On 'strict necessity', see App. No. 37138/14, *Szabó and Vissy v. Hungary*, Judgment, 12 January 2016, paras. 67, 72-73.

[138] See also *R (L) v. Commissioner of Police for the Metropolis* [2009] UKSC 3, para. 27, in which Lord Hope elucidates this point with clarity and detail. See also App. No. 24029/07, *M.M. v. the United Kingdom*, Judgment, 13 November 2012, para. 188. In *R (on the application of QSA and others) v. National Police Chiefs Council and Secretary of State for the Home Department* [2021] EWHC 272 (Admin), the High Court deemed that the policy of retaining conviction records until the perpetrators reached 100 years old was a proportionate restriction of the Article 8 right, due to the importance of having a comprehensive record of criminal convictions. In the *QSA* case, some of the claimants alleged that they were forced or groomed into sex work – prostitution being the offence in question – a fact that the court accepted (at para. 3), but this did not lead to a conclusion that the Article 8 right was violated. See also *Chief Constable of Humberside Police and others v. Information Commissioner* [2009] EWCA Civ 1079.

[139] App. No. 45325/15, *Gaughran v. the United Kingdom*, Judgment, 13 February 2020.

[140] See App. No. 74440/17, *P.N. v. Germany*, Judgment, 11 June 2020, paras. 76-90 and App. No. 14310/88, *Murray v. the United Kingdom*, Judgment, 28 October 1994, para. 93 respectively

101. In the context of data collection and/or retention, the concept of necessity creates obligations to:[141]

- Minimise – as far as reasonably possible – the amount of data collected or recorded;[142]
- Ensure the continued accuracy of the data;[143]
- Retain the data for 'no longer than necessary' to fulfil the legitimate aim for which the data was initially collected;[144]
- Limit the use of the data to the original legitimate aim; and[145]
- Operate data processing procedures and guidance that are transparent.[146]

102. Specifically, in relation to data retention, the ECtHR has adopted an approach which also depends on the factors of the case, placing particular importance on the purpose of the retention.[147] For instance, the purposes of combatting crime and preventing terrorism can be legitimate aims for interfering with the right to privacy under Article 8; however, adequate safeguards must be in place to ensure that the data processor only retains information necessary for this purpose.[148] The ECtHR's case law, in some instances, allows public authorities to store data about criminal convictions, criminal investigations, or even about mere – and vague – suspicions that an individual may be involved in criminal activity – if the government is able to meet the tests of legality, legitimate aim and necessity to achieving the aim. In assessing the necessity of data storage for these purposes, the ECtHR has considered:

- Whether the storage was limited, or indiscriminate and undifferentiated;[149]

---

[141] For more information, see Council of Europe, 'Guide to the Case-Law of the European Court of Human Rights: Data protection' (30 April 2021), paras. 103-119.
[142] App. Nos. 65286/13 and 57270/14, *Ismayilova v. Azerbaijan*, Judgment, 10 January 2019, para. 147; App. No. 25527/13, *Del Campo v. Spain*, Judgment, 6 November 2018, para. 51.
[143] App. No. 16188/07, *Khelili v. Switzerland*, Judgment, 18 October 2011, paras. 66-70.
[144] Although this does not mean that authorisations which do not set a maximum time limit are automatically unlawful; see App. No. 45325/15, *Gaughran v. the United Kingdom*, Judgment, 13 February 2020, para. 88; App. No. 8806/12, *Aycaguer v. France*, Judgment, 22 June 2017, paras. 44-46.
[145] App. No. 30083/10, *Karabeyoğlu v. Turkey*, Judgment, 7 June 2016, paras. 112-121; App. No. 44647/98, *Peck v. the United Kingdom*, Judgment, 28 January 2003, paras. 59-62.
[146] A requirement which may mandate less stringent adherence in instances where information is sensitive for national security purposes: App. No. 62332/00, *Segerstedt-Wiberg and others v. Sweden*, Judgment, 6 June 2006, para. 102.
[147] See Council of Europe, 'Guide to the Case-Law of the European Court of Human Rights: Data protection' (30 April 2021), paras. 192-227.
[148] App. Nos. 30562/04 and 30566/04, *S and Marper v. the United Kingdom*, Judgment, 4 December 2008, paras. 100-105.
[149] As above, this will depend on the person's status *vis-à-vis* the criminal justice system. If the person has not been convicted of a crime, as will often be the case with Prevent, then indiscriminate and indefinite storage is likely unlawful, as it is harder to satisfy the proportionality test. In essence, UK authorities have treated people under Prevent who are not suspected of any criminal wrongdoing in

- How long the authority stored the data;[150]
- Whether any safeguards existed to ensure the destruction or deletion of the data;[151] and
- Whether there were protections regulating third-party access to the data, and protecting the integrity and confidentiality of the information.

Oversight of Article 8 and challenging interferences

103. When considering whether public authorities can lawfully interfere with the Article 8 right, the ECtHR assesses whether the state has created independent review processes that effectively oversee whether decision-making process are fair and ensure respect for privacy rights.[152]

The person whose data the government is storing must be able to challenge – to an independent court or very court-like body – the storage, sharing and use of their data.

104. The person whose data the government is storing must be able to challenge – to an independent court or very court-like body[153] – the storage, sharing and use of their data.[154] This challenge must not simply lead to an internal review by a superior officer within the same authority that is using the personal information.[155] When the authorities decide to withhold information about personal data processing from the individual, for

much the same way it treats convicted people, regardless of the presumption of innocence: for comparison, see App. Nos. 30562/04 and 30566/04, *S and Marper v. the United Kingdom*, Judgment, 4 December 2008, paras. 119-125. In fact, the authorities, even when storing data in instances involving a crime, should have regard also to the seriousness of the offence: see App. No. 8806/12, *Aycaguer v. France*, Judgment, 22 June 2017, paras. 42-43. The law grants the Article 8 right even greater precedence in cases involving minors: see App. Nos. 30562/04 and 30566/04, *S and Marper v. the United Kingdom*, Judgment, 4 December 2008, para. 124.

[150] The length of data storage is not conclusive to a finding of a violation under Article 8, and the analysis interacts heavily with the other factors noted – principally the purpose of the retention and the existence of adequate safeguards. Indefinite data storage is usually, although not necessarily, unlawful: see App. Nos. 30562/04 and 30566/04, *S and Marper v. the United Kingdom*, Judgment, 4 December 2008; App. No. 45325/15, *Gaughran v. the United Kingdom*, Judgment, 13 February 2020; App. No. 24029/07, *M.M. v. the United Kingdom*, Judgment, 13 November 2012; App. Nos. 53205/13 and 63320/13, *Trajkovski and Chipovski v. North Macedonia*, Judgment, 13 February 2020. However, in one instance, adequate safeguards such as a review of the necessity of data storage at a minimum of every ten years rendered a claim regarding indefinite storage of data pertaining to the commission of serious offences 'manifestly ill-founded': see App. Nos. 7841/08 and 57900/12, *Peruzzo and Martens v. Germany*, Decision, 4 June 2013, paras. 44-49.

[151] Data must be easily reviewable, editable and removable: see App. No. 43514/15, *Catt v. the United Kingdom*, Judgment, 24 January 2019, para. 127.

[152] App. No. 56030/07, *Fernández Martínez v. Spain*, Judgment, 12 June 2014, para. 147; App. No. 53251/13, *A.-M.V. v. Finland*, Judgment, 23 March 2017, paras. 82-84.

[153] App. No. 9248/81, *Leander v. Sweden*, Judgment, 26 March 1987, paras. 59-84; App. No. 37138/14, *Szabó and Vissy v. Hungary*, Judgment, 12 January 2016, paras. 75-80.

[154] App. No. 964/07, *Dalea v. France*, Decision, 2 February 2010.

[155] App. No. 47143/06, *Zakharov v. Russia*, Judgment, 4 December 2015, para. 292.

instance due to ongoing surveillance, they must nonetheless implement independent oversight and safeguarding processes to ensure that they are handling the data lawfully.[156]

105. The ECtHR has long demonstrated an awareness that, where secret surveillance programmes are concerned, people may never know for sure whether the government has gathered and stored their information – which, in many domestic legal systems, makes it difficult or impossible to challenge the suspected practices in court.[157] Frequent secrecy in the national security space is one reason the Court has allowed people to challenge such secretive practices on the basis of the mere existence of the laws or policies allowing potential privacy violations to happen, if they can satisfy certain conditions.[158] The Court in *Zakharov*, a case concerning massive surveillance of communications, described its assessment process as follows:

'Firstly, the Court will take into account the scope of the legislation permitting secret surveillance measures by examining whether the applicant can possibly be affected by it, either because he belongs to a group of persons targeted by the contested legislation or because the legislation directly affects all users of communication services... Secondly, the Court will take into account the availability of remedies at the national level and will adjust the degree of scrutiny depending on the effectiveness of such remedies...'[159]

106. Additionally, the Court explained that:

'Where domestic law does not indicate with sufficient clarity the scope and manner of exercise of the discretion conferred on the domestic authorities to collect and store in a surveillance database information on persons' private lives – in particular, where it does not set out in a form accessible to the public any indication of the minimum safeguards against abuse – this amounts to an interference with private life as protected by Article 8 § 1 of the Convention.' [160]

For instance, in *Varga v. Slovakia*, the ECtHR found that the lack of clarity around procedural safeguards and the decision-makers' broad discretion when it came to data collection and storage violated Article 8(1).[161]

[156] App. No. 47143/06, *Zakharov v. Russia*, Judgment, 4 December 2015, para. 234; App. No. 5029/71, *Klass and others v. Germany*, Judgment, 6 September 1978, paras. 55-59.
[157] App. No. 5029/71, *Klass and others v. Germany*, Judgment, 6 September 1978, paras. 36, 48.
[158] App. No. 47143/06, *Zakharov v. Russia*, Judgment, 4 December 2015, paras. 171-172.
[159] App. No. 47143/06, *Zakharov v. Russia*, Judgment, 4 December 2015, para. 171.
[160] Council of Europe, 'Guide on Article 8 of the European Convention on Human Rights' (31 August 2021), para. 213, referencing App. No. 30194/09, *Shimolovs v. Russia*, Judgment, 21 June 2011, para. 66.
[161] App. No. 58361/12, 25592/16 and 27176/16, *Varga v. Slovakia*, Judgment, para. 162.

6. Concerns and possible illegalities regarding data processing under Prevent

We conclude that the UK government has failed to establish that data processing under Prevent is 'necessary'. As a result, we believe that Prevent-related data processing in the UK is unlawful.

107. Data collection, processing, sharing and storage as part of Prevent raise a number of legal issues, under both UK law and the ECHR. We analyse each of these in more detail in this section, before concluding that, when the Home Office and other government bodies advise public officials to pedantically follow official guidance, this could lead to systemic and widespread law-breaking. More specifically, we conclude that the law is insufficiently clear and precise to meet the ECHR's requirements that any interference with the right to privacy must be made 'in accordance with the law'. Further, we conclude that the government has failed to establish – through evidence – that data processing under Prevent is 'necessary'. As a result, we believe that Prevent-related data processing in the UK is unlawful.

108. Further, there appears to be a general disagreement or lack of clarity among professional bodies, government departments and practitioners charged with implementing Prevent about how the latter should treat personal data under the strategy. While this report has set out some examples of policies, statutory guidance and practices that – at least in theory – give weight to human rights and data protection principles, there are many others that apparently do not (or might not). The conflicting nature of the advice likely makes it difficult to implement in practice; when doing so, it is possible that many professionals will err on the side of caution[162] – sharing and processing people's personal data in breach of human rights and data protection laws. As we will note throughout this section, the general lack of transparency in Prevent-related data processing by UK public authorities may – as well as itself running afoul of the ECHR – also contribute to other potential law-breaking under the country's own data protection laws.

European Convention on Human Rights

Interference

109. In assessing the legality of Prevent-related restrictions on the right to private and family life – through data processing – we must first assess whether these actions amount to an interference with the Article 8 right. If so, for the data processing to be lawful, authorities must act in accordance with the law (both UK and international law), and the restrictions on privacy must be necessary to reaching a legitimate aim. We will now discuss each of these elements.

---

[162] See, for instance, Lee Roy Beach and Terence R. Mitchell, 'A Contingency Model for the Selection of Decision Strategies' (1978) 3(3) Academy of Management Review 439; James W. Dean, Jr. and Mark P. Sharfman, 'Does Decision Process Matter? A Study of Strategic Decision-Making Effectiveness' (1996) 39(2) Academy of Management Journal 368; TJ Stewart, 'A critical survey on the status of multiple criteria decision making theory and practice' (1992) 20(5-6) Omega 569; Terence O'Sullivan, *Decision Making in Social Work* (Bloomsbury: Red Global Press, 2nd edn, 2010), p. 34.

110. In the context of Prevent, as outlined above, it appears that information regarding a person's name, address, and religious or other beliefs are at a minimum shared among public authorities and stored in relevant databases; it is likely that other such information is also stored or shared. To us, it seems clear that the Court would view the storage, use, and sharing of such personal data as an interference the Article 8 right.

Legality

111. As noted above, data protection legislation in the UK regulates the processing of Prevent-related personal data. For instance, processors share Prevent-related data on grounds of the statutory Prevent duty, and under other safeguarding-related duties,[163] or otherwise in the public interest. However, it is often unclear which specific grounds authorities are relying upon when they process or share data, and in many instances the policies UK data processors use for Prevent purposes are not publicly available. For instance, a local authority may refer an individual to Prevent – sharing their personal data with several other public bodies – but not inform the person who was referred. Later, once the referred person finds out about the referral, they have no way of knowing why they were referred, nor how the decision to refer was made.

112. The police additionally have distinct powers for data collection and retention; in summary:

'At common law the police have the power to obtain and store information for policing purposes, i.e. broadly speaking for the maintenance of public order and the prevention and detection of crime. These powers do not authorise intrusive methods of obtaining information, such as entry upon private property or acts (other than arrest under common law powers) which would constitute an assault...' [164]

113. These broad powers are then limited in practice by data protection laws and human rights legislation.

114. However, as noted throughout this report, government policies and official guidance – and perhaps, by extension, the precise demarcation of public authorities' data sharing powers – are often neither clear nor accessible where Prevent is concerned.[165] Additionally, again as noted throughout this report, it appears that in many instances, the government relegates the individual's Article 8 rights in official guidance to having minimal importance – an attitude likely also reflected in practice, if the written policy is any indication. Finally, the national government's and other public bodies' over-reliance on policies and statutory guidance for regulating Prevent-related data processing – as opposed to laws passed by Parliament – itself calls into question compliance with human rights laws. We argue that, taken individually, each of these concerns may

[163] Care Act 2014, s42.
[164] *R (Catt) v. Association of Chief Police Officers of England, Wales and Northern Ireland* [2015] UKSC 9, para. 7.
[165] UK courts have held that data collection powers in the UK have not been implemented 'in accordance with law' due to unlawful delegation of powers: see *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and others*, IPT/15/110/CH, 23 July 2018.

infringe Article 8's legality requirement; however, when combined, we conclude that the UK's practice is unlawful under the ECHR.

Most UK public bodies' data processing policies for Prevent are not publicly available.

115. First, we note that, although the broad legal framework is publicly available, many of the policies and guidelines that data processors follow when engaging in Prevent-related data processing are not. Throughout the course of conducting research for this report, we have found that, although statutory guidance exists through which the Home Office and other government departments tell public bodies how to process Prevent data, most public bodies' data processing policies are not publicly available.

When a public body holds on to personal data for too long, the risk of a data breach, improper access or sharing, illegal uses, failures to keep the information accurate, and other problems may increase.

116. We also believe that laws and policies around the processing of Prevent-related data are insufficiently clear and precise. One example is the law relating to time limits for the retention of personal data. The UK GDPR provides an overview of the applicable law, requiring that 'personal data shall be … kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed…', while 'appropriate time limits must be established for the periodic review of the need for the continued storage of personal data'.[166] However, this law does not actually explain how long organisations, including public authorities, should hold on to personal data; instead it is up to the controlling agency to take and justify its own decisions to store data.[167] The Home Office's guidance does little to supplement this vague law; instead, it only refers to the data sharing process, and not what happens to this personal data after the referral. Given this lack of precision, we believe it is very likely that practitioners are likely to unlawfully hold on to personal data for unnecessarily long periods of time, as the Court held in the *II* case. When a public body holds on to personal data for too long, the risk of a data breach, improper access or sharing, illegal uses, failures to keep the information accurate, and other problems may increase.

117. This situation is not consistent with the ECHR, which requires a clear, specific explanation – in a publicly available law – of the circumstances in which private information may be collected or shared, and limits on how it is treated.

118. There is evidence that this lack of clarity leads to problems in practice, as practitioners and authorities remain unsure or potentially misguided about how to implement Prevent-related law and policy in line with their human rights and data protection obligations.

[166] See Article 5(e); Data Protection Act 2018, s39(2).
[167] Information Commissioner's Office, 'Principle (e): Storage limitation' (*ICO*).

119. Based on interviews with health professionals for its 2020 report *False Positives: the Prevent counter-extremism policy in healthcare*, the non-profit organisation Medact argues that the introduction of Prevent caused an expansion of the grounds for lawful sharing of patient data without the patient's express or implied consent. According to Medact, this occurred despite official guidance to the contrary from the British Medical Association.[168] The report's discussion shows a lack of clarity in the policies and related materials:

'[S]ome official Prevent training materials appear to actively discourage health workers from seeking informed consent from patients, as well as fudging the crucial difference between disclosures made for the purpose of safeguarding and disclosures justified in the public interest. Finally, while the Prevent duty only applies to organisations, Prevent training materials inaccurately present individual clinicians themselves as legally responsible for reporting suspicions about radicalisation. As a result, many health workers believe they may be held individually accountable for failing to refer, which creates pressure and in some circumstances leads to a "rush to refer".'[169]

120. In its guidance, the government dedicates much more space to monitoring and enforcement – or to 'risks' that an individual may be drawn into terrorism – than to ensuring lawful, voluntary, and consensual referrals in the first instance.[170] Again, this points to a failure to ensure legality by creating and publicising clear, specific laws and regulations.

121. Illustrating the lack of clarity, some Prevent-related data sharing practices may violate professional guidance and standards. Medact's report notes that:

'…When Prevent was placed on a statutory footing in 2015, the British Medical Association declared in guidance to members that the policy did not alter these circumstances [in which practitioners could share information without a patient's consent]. However, in practice there are worrying indications that Prevent has eroded and undermined the expectation of confidentiality.[171] *[footnotes omitted]*

122. Likewise, the DfE's guidance occasionally refers the need to abide by privacy regulations to ensure that practitioners do not share personal data unnecessarily. However, elsewhere in the DfE's guidance we see the body steering practitioners toward making referrals to Prevent even when they are concerned that doing so may violate the individual's right to privacy. For instance, one of the body's guides contains

---

[168] Hilary Aked, 'False Positives: the Prevent counter-extremism policy in healthcare' (*Medact*, 2020), p. 54.
[169] Hilary Aked, 'False Positives: the Prevent counter-extremism policy in healthcare' (*Medact*, 2020), p. 54.
[170] Home Office, 'Revised Prevent duty guidance: for England and Wales' (*Gov.uk*, 1 April 2021), paras. 23-28, 52-56, 72-76, 96-98, 132-136, 145; Home Office, 'Prevent duty guidance: for further education institutions in England and Wales' (*Gov.uk*, 1 April 2021), paras. 29-31; Home Office, 'Prevent duty guidance: for higher education institutions in England and Wales' (*Gov.uk*, 1 April 2021), para. 31; HM Government, 'Channel Duty Guidance: Protecting people vulnerable to being drawn into terrorism' (2020), paras. 109-117.
[171] Hilary Aked, 'False Positives: the Prevent counter-extremism policy in healthcare' (*Medact*, 2020), p. 54.

a 'myth-busting' factsheet on information sharing which assures practitioners that data protection and human rights legislation do not prohibit data sharing.[172]

123. If practitioners and experts are unsure of the rationale for – and limits on – data sharing and storage, then it is difficult to argue that they have effectively mainstreamed human rights and data protection laws in decision-making. For instance, dedicated Channel mentors – the professionals responsible for managing individuals referred to Prevent – have also informed on their clients to the police, despite Home Office officials criticising this use of personal data as contrary to the purpose of the Channel process and Prevent as a whole.[173]

124. In any case, as emphasised throughout this report, it appears likely that authorities and data processors side-line human rights and data protection principles in both policy and practice – breaching international and domestic laws.

125. Other policies are vague, and practitioners may interpret them inconsistently. For example, the NHS's guidance telling NHS trusts to create 'robust' data sharing practices partly hinges on how practitioners interpret the term 'robust', without explaining whether a 'robust' procedure is one that includes compliance with human rights and data protection laws. Certainly, any Prevent guidance implying that practitioners should not allow these laws to stand in the way of a referral raise concerns about legality for purposes of the ECHR.

126. The uncertainty regarding the grounds for processing personal data under Prevent also creates difficulties in practice, as disclosures required by law grant less priority to consent (instead, the government advises that processors should disclose the fact of sharing to the individual after they have shared the data), whereas disclosures in the public interest appear, at least in statutory guidance, to prioritise obtaining the individual's informed consent.[174] This may lead to divergent outcomes in similar cases: if the authority believes it is referring an individual to Prevent as a legal requirement, then it is unlikely to seek the person's consent; by contrast, if the authority believes it is referring an individual to Prevent in the public interest, it may be more likely to seek consent.

127. In any event, a policy is not a law, and we conclude that the existing lack of specific laws – compounded by unclear or even conflicting policies – violates Article 8 of the ECHR.

Legitimate Aim

128. Under Article 8, we must also assess whether the government has a legitimate aim for interfering with privacy by collecting, storing and sharing Prevent data. Of the aims

[172] HM Government, 'Working Together to Safeguard Children: A guide to inter-agency working to safeguard and promote the welfare of children', p. 21.
[173] Richard Kerbaj, 'Anti-extremism mentors inform on clients to police' (*The Sunday Times*, 11 August 2019).
[174] For instance, see the distinction in the British Medical Association's guidance: British Medical Association, 'Confidentiality toolkit: A toolkit for doctors' (1 July 2021), pp. 11-17.

permitted by the ECHR, the most relevant in the Prevent context are exceptions related to national security and the prevention of crime or disorder.

It is possible that the UK is sharing Prevent-related personal data with other countries for intelligence purposes – ones that may be unrelated to preventing violence or other crime.

129. In practice, the ECtHR tends to afford governments a large 'margin of appreciation' in determining the existence of a legitimate aim. For present purposes, we believe the UK government could successfully claim a legitimate aim under one of these grounds, as we do not have evidence to suggest that the UK government has authorised the processing of Prevent-related personal data in pursuance of an ulterior motive. Indeed, such an approach would appear to be reminiscent of the ECtHR's approach in *Kaushal*, in which the Court accepted that counter-extremism measures would fall within the national security aim.[175] We note with concern, however, the possibility that the UK is sharing Prevent-related personal data with other countries for intelligence purposes – ones that may be unrelated to preventing violence or other crime.

Necessity

130. Although the ECtHR grants governments a wide 'margin of appreciation' in relation to the existence of a legitimate aim, the Court has shown greater strictness in its assessments of whether interferences with privacy are *necessary* to achieving that aim.

131. It is our view that, in the context of Prevent-related data processing, the government's case for necessity is weak. To put it bluntly, the government has not established a sufficient evidence base to justify data gathering, storage and sharing under Prevent as effective in – let alone necessary to – stopping acts of terrorism; it has refused to publish some of the supporting evidence it does claim to have.[176] Additionally, the confusion within the government and public authorities about the purpose of Prevent-related data sharing argues against the idea that the sharing is necessary.

If there is little or no reason to believe Prevent 'works', or that it is the least intrusive possible method, then there is similarly little reason to believe it is necessary to achieving its stated aims.

132. Several criminologists and other academic commentators have called into question the evidentiary basis for Prevent, and more broadly, the purported links between

[175] App. No. 1537/08, *Kaushal and others v. Bulgaria*, Judgment, 2 September 2010, para. 28.
[176] The Prevent strategy is underpinned by the 'Extremism Risk Guidelines' or 'ERG22+': see Beverly Powis, Kiran Randhawa-Horne and Darren Bishopp, 'The Structural Properties of the Extremism Risk Guidelines (ERG22+): a structured formulation for extremist offenders' (Ministry of Justice, 2019). For critique, see Alice Ross, 'Academics criticise anti-radicalisation strategy in open letter' (*The Guardian*, 29 September 2016); Gabriel Gray Mythen and Evelyne Baillergeau, 'Considering strategies designed to counter radicalisation: Comparative reflections on approaches in the United Kingdom and Belgium' (2021) 11(5) Oñati Socio-legal Series 1133.

holding 'extremist' beliefs and actually engaging in terrorism or other crime.[177] In other words, the government has not established that data collection and sharing under Prevent 'works', or can reasonably be expected to work, based on objective evidence. If there is little or no reason to believe Prevent 'works', or that it is the least intrusive possible method that works, then there is similarly little reason to believe Prevent is necessary to achieving its stated aims.

133. Moreover, rather than stating that processors can only share personal data when necessary to reach the government's purported legitimate aim under Prevent, official guidance instead suggests to practitioners that they must not let human rights concerns stand in the way of a Prevent referral. That is, the government does not appear to require that the data collection, storage or sharing be necessary.

134. Current practice also shows us that many data processors take an approach to data processing that goes beyond necessity, as evidenced by the MPS's submissions in the *II* case. In that case, the MPS argued that it should be able to store an erroneous Prevent referral on an individual's file for at least six years, as 'radicalisation is considered to be a process that occurs over time' and that 'where there is plainly a legitimate aim in retaining data for the purpose of preventing terrorist activity, we consider that retention for [this period of time]… is proportionate'.[178] This view skips the step of considering whether retaining mistaken information is *necessary*, and we believe the Court would likely disagree with such a view. In general, there appears to be little reason to believe that wrong information is useful, let alone necessary, to achieving any legitimate aim. To the contrary, wrong information would appear to detract from any legitimate goal by creating distractions, wasting resources and creating a risk of further errors.

135. The People's Review of Prevent, an independent review of Prevent focusing on the views of people with lived experience of the strategy, suggested in a 2022 report that data collection under Prevent is over-inclusive, reflecting high percentages of referrals that ultimately get dismissed and resulting in 'the widespread capture and retention of data of non-criminals on criminal databases.'[179] According to this report, the police and other public authorities also store the data of children without their consent or knowledge (or that of their family or legal guardians), regardless of the commission of a criminal offence or the progress of a Prevent referral – even if the authorities subsequently classify a referral as 'mistaken'.[180] The report states:

---

[177] In relation to national security grounds, see the useful illustration in App. Nos. 38334/08 and 68242/16, *Anchev v. Bulgaria*, Decision, 5 December 2017, paras. 92-116. On the link between terrorism and extremism, see Recep Onursal and Daniel Kirkpatrick, 'Is Extremism the 'New' Terrorism? the Convergence of 'Extremism' and 'Terrorism' in British Parliamentary Discourse' (2021) 33(5) Terrorism and Political Violence 1094; Astrid Bötticher, 'Towards Academic Consensus Definitions of Radicalism and Extremism' (2017) 11(4) Perspectives on Terrorism 73.

[178] *R (on the application of II (by his mother and Litigation Friend, NK)) v. Commissioner of Police for the Metropolis* [2020] EWHC 2528 (Admin), para. 56.

[179] John Holmwood and Layla Aithadj, 'The People's Review of Prevent' (February 2022), pp. 55-56, 99-114.

[180] The report sets out multiple examples: see John Holmwood and Layla Aithadj, 'The People's Review of Prevent' (February 2022), pp. 64, 89-90, 95-96, 99-114.

'One of the consequences of securitising safeguarding under Prevent, is that children are interacting with the criminal system despite no criminal offence having occurred, nor having been intended. The process of an individual passing from being suspected by, say, their teacher, of showing signs of extremism, to being placed on Channel if the Prevent referral follows through to completion, involves a number of data collection points. At each of these points, information about a child or young person is recorded and potentially retained, and it can be shared with the other agencies with which Prevent procedures intersect.' [181]

136. Finally, it also appears that third parties may have unnecessary access to stored Prevent data. This report has described the use of centralised databases for Prevent referrals, which remain accessible by a range of government agencies, as well as the government's and public authorities' tendency in official Prevent guidance and training to emphasise the desirability of extensive data sharing – without placing limits based on necessity. It also appears likely that data is shared with other government departments – such as with the Home Office for immigration purposes, and to other police forces for law enforcement – outside of the safeguarding purpose of the original Prevent referral. We conclude that the government has not shown that this data sharing in general is strictly necessary, or that it has created limits sufficient to ensure that any access to people's data in specific cases is necessary.

Data protection legislation

137. Before engaging in a detailed application of the data protection laws, we must first determine what law applies: does the law relating to law enforcement apply in this context? And do the provisions governing the intelligence services also apply? The answer to each of these questions is straightforward. First, although law enforcement authorities do hold Prevent-related functions, Prevent is not a means of enforcing the criminal law. Instead, Prevent operates to counter 'extremism' – a set of beliefs that it is not illegal to hold. (Under human rights law, the freedoms of thought, opinion and belief are absolute.) Likewise, although the police also have safeguarding functions, these do not fall within the 'law enforcement' provisions of the DPA, as Prevent aims to safeguard individuals rather than the general public.[182] Indeed, in *Butt*, the authorities did not appear to rely on the laws that apply to police when they engage in data processing under Prevent.[183]

138. This means that the DPA's provisions on law enforcement will only apply when Prevent-related data is subsequently processed for the purposes of law enforcement.[184]

---

[181] The report sets out multiple examples: see John Holmwood and Layla Aithadj, 'The People's Review of Prevent' (February 2022), p. 99.
[182] Data Protection Act 2018, s31 defines 'law enforcement purposes' as 'purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.'
[183] *R (Butt) v. Secretary of State for the Home Department* [2019] EWCA Civ 256, paras. 122-130. This also correlates with the definition of Prevent as a safeguarding policy: see National Chiefs' Council, 'Delivering Prevent: The role of police in this safeguarding programme' (*NPCC*).
[184] See *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. 80-88.

139. However – although these institutions are not the focus of this report – as the provisions relating to data processing by the intelligence services contain no purpose limitation, Part 4 of the DPA would apply to Prevent-related data processing by the Security Service, the Secret Intelligence Service and GCHQ. We need further information about how the intelligence services engage in Prevent-related data collection and processing before we can conclude whether these practices comply with the requirements listed in Part 4 of the DPA. This need for further information highlights the fact that the laws are not clear, in violation of the ECHR (see above).

140. In the general context – that is, data not used by the intelligence services or for law enforcement purposes – it is likely that Prevent-related law and policy set the stage for law-breaking. For instance, the transparency obligation requires that data processors be clear about how they process personal data,[185] while the accountability obligation mandates the creation of internal processes to ensure compliance with data protection law.[186] As outlined above, Prevent-related data processing guidelines and procedures are often not publicly available, meaning that people often do not know that authorities have stored or shared their personal data. This secrecy may also limit accountability when laws and processes are not complied with.

141. Additionally, the purpose limitation obligation requires that organisations be transparent about how they use personal data and that they only use this data for its initial intended purpose,[187] while the fairness requirement means that organisations must use personal data in a foreseeable way.[188] In the context of Prevent, this means that the actors involved in a Prevent referral can only use the data they collect for the purpose of the referral process – not for other purposes. However, the research summarised above indicates that public bodies in the UK may be sharing Prevent-related data with the Home Office, for immigration purposes, with the police, to aid in law enforcement, and also with education providers, to assess whether and how they engage with current or potential students. Each of these purposes appear to be outside the scope of the original Prevent referral and may break the law. To share the data legally, the authority should obtain additional consent – or rely on an additional legal ground – before changing the purpose of the data collection or sharing.

142. In terms of the grounds for data processing under Prevent, as many of the authorities engaging in data processing under Prevent are subject to the Prevent duty – which requires them to 'have due regard to the need to prevent people from being drawn into terrorism'[189] – authorities could argue that data processing is an extension of their statutory function. This would mean they would not need to obtain the person's consent to the data collection and storage.

143. However, the data collection and storage could still be illegal, since the data protection legislation requires processors to apply further protections to much of the information that authorities process for the purposes of Prevent – such as data

[185] Information Commissioner's Office, 'Transparency' (*ICO*).
[186] Information Commissioner's Office, 'Accountability and governance' (*ICO*).
[187] Information Commissioner's Office, 'Principle (b): Purpose limitation' (*ICO*).
[188] Information Commissioner's Office, 'Principle (a): Lawfulness, fairness and transparency' (*ICO*).
[189] Counter-Terrorism and Security Act 2015, s26.

revealing religious or philosophical beliefs and political opinions.[190] In the absence of consent, the authorities might not have a sufficient legal basis for the ways they are handling the data, especially when the data is sensitive. For such special categories of personal data, s10(b) authorises processing of this data on the grounds of 'substantial public interest', which means that public authorities must believe there is an even greater justification for interfering with a person's privacy, than when 'regular' – that is, non-sensitive – personal information is involved. Moreover, the DPA requires that processing of this special category data must have a basis in UK law. Additionally, processors must be able to show that the processing meets one of the conditions in Part 2 of Schedule 1, which includes 'statutory… and government purposes', and for 'safeguarding of children and of individuals at risk'.[191] (As noted above, authorities may argue that the statutory Prevent duty meets these two conditions.) Finally, an authority that wants to process special personal data may need to create an 'appropriate policy document', outlining how the authority treats this data, and how decision-makers will comply with the data protection principles; the law also requires processors to explain why consent has not been sought in individual cases.

144. In the *Butt* case, the Court of Appeal concluded that the processing of data for the purposes of Prevent had a legal basis because it was a legitimate exercise of functions of the Crown,[192] and because the claimant had already made the information about his views – which was the personal information stored in relation to Prevent – public.[193] Even if the Court of Appeal was correct in *Butt*, we can distinguish this case from other instances where authorities store more sensitive – and not otherwise publicly available – information. Additionally, the Court's conclusions in *Butt* might not apply to authorities other than a government department – such as schools, NHS trusts and police services.

145. Again, the statutory Prevent obligation will provide arguable legal authority for public bodies to process personal data for Prevent purposes. Other public bodies may seek to rely on Prevent's definition as a safeguarding regime as their legal authority for processing sensitive personal data. If authorities successfully make these legal claims, they will not have to provide evidence that they are processing sensitive personal data with a 'substantial public interest' in mind.[194] However, public authorities must still ensure that they have an 'appropriate policy document' explaining how and in what circumstances sensitive personal data may be processed. Authorities seeking to rely on safeguarding as their legal authority for data processing must explain why they cannot obtain the individual's consent, when they do not do so.

146. As explained elsewhere in this briefing, the government and public authorities advise practitioners to share large amounts of personal data with few limitations, and do not

[190] For an practical guide, see Information Commissioner's Office, 'Special category data' (*ICO*).
[191] Data Protection Act 2018, Schedule 1, paras. 6 and 18 respectively; see also General Data Protection Regulation, Article 9(g).
[192] Data Protection Act 2018, Sch. 2, para. 5.
[193] Data Protection Act 2018, Sch. 3, para. 5; *R (Butt) v. Secretary of State for the Home Department* [2019] EWCA Civ 256, paras. 126-128.
[194] For an overview, see the table at Information Commissioner's Office, 'What are the substantial public interest conditions?' (*ICO*).

provide additional protections for sensitive personal data. We therefore believe that Prevent-related data processing could be legally challenged for failing to comply with data protection legislation.

147. When public bodies receive Prevent-related data for reasons other than Prevent – for example, when police receive Prevent data for law enforcement purposes, or when the Home Office receives it for immigration purposes – there may also be practical concerns about whether the original legal grounds for the data processing extend to these new activities.[195] For instance, if a person voluntarily agrees to the Channel process, during which an authority shares their personal data with the Home Office, does the Home Office then have a legal basis to use or share that data for immigration-related purposes, which would be beyond the scope of the initial consent?

148. While data protection legislation contains a 'national security' exemption to some of the data protection principles, which could be applicable in the Prevent context, this does not remove the obligation on processors to have a legal ground for any personal data processing. As outlined above, it is likely that some practitioners engaging in Prevent-related data processing have not complied with these grounds.

149. Additionally, it is possible that data processors are retaining personal data for longer than is allowed under data protection legislation. The three circumstances under data protection legislation in which processors may store personal data indefinitely are archiving in the public interest, scientific or historical research, and statistical research. Evidently, therefore, indefinite storing of personal data under Prevent would fail to satisfy any of these exceptions. Although we are not aware of any confirmed examples of indefinite storage of Prevent-related data, official guidance and practice, as outlined elsewhere in this report, tends towards lengthy and potentially arbitrary data retention periods. This itself could violate data protection law.

7. Preliminary conclusions

150. While publicly available information regarding data processing practices for Prevent is sparse, with authorities publicising guidance on a piecemeal basis, we can nonetheless draw some preliminary conclusions about the legality of what UK authorities are doing.

Rather than placing people's legal rights at the forefront of decision-making, the government errs on the side of collecting and sharing more data about more people.

151. From the evidence outlined above – the policies, practices and training that apply to public bodies – a trend emerges. Rather than placing people's legal rights at the forefront of decision-making, the government – and by extension other authorities

[195] Katja Lindskov Jacobsen, 'Biometric data flows and unintended consequences of counterterrorism' (2021) 103 International Review of the Red Cross 619, p. 638

implementing Prevent – errs on the side of collecting and sharing more data about more people. In practice, this approach could create widespread illegality.

152. At a minimum, the lack of clear, specific laws authorising and constraining data collection, storage and sharing under Prevent violates the 'legality' requirement of Article 8 of the ECHR, in our view. We believe this problem is obvious and that the ECtHR would very likely agree.

The approach the UK government takes under Prevent is far too opaque and often based on muddled guidance rather than publicly available statutes. Worse, the available guidance sometimes explicitly downplays people's privacy and data protection rights, which are legally binding.

153. While we recognise that governments cannot always act in a completely transparent manner when engaged with security, including when processing personal data, we argue the approach the UK government takes under Prevent is far too opaque and often based on muddled guidance rather than publicly available statutes. Worse, the available guidance sometimes explicitly downplays people's privacy and data protection rights, which are legally binding. While some authorities may have created safeguards to ensure that they comply with their legal obligations under data protection and human rights laws, the *I/* case illustrates that in many instances, decision-makers appear to underestimate the importance of these laws.

154. Furthermore, the piecemeal and confusing legal and policy framework makes it difficult for anyone to foresee how a particular authority could handle their data.

155. We also conclude, based on the research described above, that the government and public bodies often advise data processors to use personal data in circumstances that likely go far beyond what is necessary. Moreover, the government has never shown that the Prevent scheme in general is effective in achieving its stated aims, let alone necessary. These facts suggest to us that the government and individual authorities are also violating the 'necessity' requirement of Article 8 ECHR.

156. As well as our conclusions about compliance with human rights laws, we also conclude that public bodies' data processing practices may be breaching UK data protection legislation, particularly as data is processed in secret and without sufficient oversight. Additionally, many authorities appear to store this data for longer than is necessary. While individual public authorities would be responsible for any breaches of UK data protection laws, we believe the government holds central responsibility for preventing this. Throughout this report, we demonstrate how the centrally drafted law and guidance on Prevent is often contradictory and generally inadequate to ensure that data processors comply with their data protection obligations.

First published in 2022
by Rights and Security International
465c Hornsey Road, London N19 4DR

London
WC1A 2RP
United Kingdom

www.rightsandsecurity.org

Rights & Security International (RSI) is a London-based NGO with over 30 years of experience in ensuring that measures governments take in the name of national security respect human rights. This report aims to bolster joint advocacy efforts for the creation of oversight mechanisms to ensure the UN's respect for human rights when it acts in the name of counter-terrorism.

This report was researched and drafted by Jacob Smith, UK Accountability Officer at Rights & Security International, with valuable research assistance from intern Dominique Argüelles. Review was provided by Sarah St Vincent, Executive Director, and Tufyal Choudhury, Principal Legal Adviser. Sabah Hussain, Migration, Citizenship and Communications Officer, formatted and published the report.

Cover photo: International flags
Source: Unsplash.com

Report design by Susak Press
daniel@susakpress.com

Visit us at **www rightsandsecurit org**
and follow our work on Twitter **rightssecurit**

RIGHTS & SECURITY INTERNATIONAL