Protection of Freedoms Bill

Briefing for House of Commons Second Reading

March 2011

For further information contact

Eric Metcalfe, Director of Human Rights Policy

email: emetcalfe@justice.org.uk direct line: 020 7762 6415

JUSTICE, 59 Carter Lane, London EC4V 5AQ tel: 020 7329 5100

fax: 020 7329 5055 email: admin@justice.org.uk website: www.justice.org.uk

Introduction

1. Founded in 1957, JUSTICE is a UK-based human rights and law reform organisation. Its mission is to advance justice, human rights and the rule of law. It is also the British section of the International Commission of Jurists.

2. JUSTICE welcomes the Protection of Freedoms Bill as an important step in reversing many of the unnecessary and disproportionate measures introduced by the previous government. There is much in the Bill we welcome and little in it with which we would in principle disagree. However, we have also identified a number of problems with several provisions, whether it be a lack of detail (e.g. clauses 29-36) , improper reliance on Henry VIII clauses (e.g. clauses 39-53), or a failure to provide sufficient safeguards against abuse (e.g. clauses 58-62).

3. More generally, we are concerned that many of the measures indicate a piecemeal approach to problems in areas where more fundamental, root-and-branch reform has long been overdue. For example, much of the Bill address such issues as surveillance, data retention and privacy, including amendments to the Regulation of Investigatory Powers Act 2000. In addition to the existing oversight of surveillance and privacy matters provided by the Interception of Communications Commissioner, the Information Commissioner, the Surveillance Commissioners and the Intelligence Services Commissioner, the Bill proposes the addition of a Commissioner for the Retention and Use of Biometric Material (clause 20) and a Surveillance Camera Commissioner (clause 34). While there is an overwhelming case for further safeguards to be introduced in these areas, we do not believe that the creation of additional Commissioners is necessarily the best way forward.

4. Indeed, several parts of the Bill would be improved by introducing the requirement for prior judicial authorisation of executive action. We note that the importance of independent judicial control has already been accepted by the Coalition government: clauses 37 and 38 of the Bill require local authority authorisations to be approved by a magistrate. However, surveillance by local authorities is far from the only area in which effective judicial control is lacking. The proposed replacement for section 44 of the Terrorism Act 2000 is another provision in which prior judicial authorisation would prove a vital check against the arbitrary use of stop and search powers. Such a step would not only help secure compliance with the right to privacy under article 8 of the European Convention on Human Rights but it would also be consistent with the UK's own constitutional traditions. After all, British judges have had centuries of experience with issuing warrants for a wide range of intrusive activities by the executive, e.g. search warrants.

5. Therefore, although the Bill represents an important first step, it also shows that the protection of our freedoms will require not just a single piece of legislation, but continued reform.

Clauses 1-25 - Destruction, Retention, Use of Fingerprints etc

6. In its programme for government published in May last year, the Coalition promised to 'adopt the protections of the Scottish model for the DNA database'.[1] JUSTICE had previously recommended the adoption of this model, which was described by the Grand Chamber of the European Court of Human Rights in *S and Marper v United Kingdom* in December 2008 as follows:[2]

> Under the 1995 Criminal Procedure Act of Scotland, as subsequently amended, the DNA samples and resulting profiles must be destroyed if the individual is not convicted or is granted an absolute discharge. A recent qualification provides that biological samples and profiles may be retained for three years, if the arrestee is suspected of certain sexual or violent offences even if a person is not convicted (section 83 of the 2006 Act, adding section 18A to the 1995 Act.). Thereafter, samples and information are required to be destroyed unless a Chief Constable applies to a Sheriff for a two-year extension. (para 36)

7. By contrast, the Grand Chamber noted, England, Wales and Northern Ireland were the 'only jurisdictions within the Council of Europe to allow the indefinite retention of fingerprint and DNA material of any person of any age suspected of any recordable offence'.[3] The Court found this indefinite detention failed to strike 'a fair balance between the competing public and private interests' involved and this amounted to 'a disproportionate interference with the … right to respect for private life', one that could not 'be regarded as necessary in a democratic society'.[4]

8. Following that judgment, Parliament enacted a new retention scheme under sections 14 to 23 of the Crime and Security Act 2010. However, JUSTICE opposed that scheme in its parliamentary briefings on the Bill on the basis that no evidence had been put forward by the government to show that the Scottish model was disproportionate. We continue to believe that the Scots legislation strikes a proper balance between public and private interests, by allowing limited retention for those suspected of sexual and violent offences, with further extension by judicial authorisation only.

---

[1] *The Coalition: Our Programme for Government* (Cabinet Office, May 2010), p11.

[2] *S and Marper v United Kingdom* (4 December 2008, Applications nos. 30562/04 and 30566/04), para 36.

[3] Ibid, para 110.

[4] Ibid, para 125.

9. As annex B of the explanatory notes make clear, the clauses in the current Bill do not exactly replicate those in the Scottish Act. Some of the differences are positive, while several are not.

Clause 3 – persons arrested for or charged with a qualifying offence

10. The retention scheme in clause 3 draws a distinction between those arrested and those charged with a qualifying offence. Although both groups are liable to have their DNA profile retained for a further 3 years (extendable by a further two years), those who have been arrested but not charged are only liable to have their profile retained if the Retention of DNA Commissioner agrees (subclauses 63F(5)(c) and (11), as inserted by clause 3). It is unclear in this context why persons charged but not convicted should be treated differently than persons arrested but not charged. No such distinction appears in the corresponding Scottish legislation. If the Commissioner is to have a role in relation to arrested persons, we see no reason why this should not be extended to those charged but not convicted. More generally, we take the view that prior judicial authorisation is typically a better mechanism for dealing with these kinds of questions than the establishment of specialist Commissioners.

11. In addition, the explanatory notes claim that the Bill goes further than in Scotland by permitting only a single extension to the statutory period of retention. However, if this is indeed the government's intention, we suggest that this should be made explicit on the face of the Bill as we do not read subclauses 63F(7)-(10) (as inserted by clause 3) as preventing multiple applications for extension.

Clause 7 – Persons under 18 convicted of first minor offence

12. Clause 7 provides for the destruction of DNA profiles of youth offenders convicted of minor crimes after five years,[5] where it was their first offence.[6] We regard this as an improvement on the Scottish model.

Clause 8 – Persons given a penalty notice

13. Where a person has been arrested and subsequently receives a fixed penalty notice rather than being charged, clause 8 allows for the retention of their DNA profiles for a period of 2 years. In light of our opposition to the increasing use of penalty notices, particularly against young people, we are concerned that this provision will unduly expand the National DNA Database. In particular, we believe it should be made clear that persons who contest a penalty

[5] Not including the period of any custodial sentence. If the offender receives a custodial sentence greater than 5 years, the DNA profile can be retained indefinitely (clause 63J(3)).

[6] Clause 63J(5).

notice and are subsequently acquitted will not be liable to have their DNA profile or fingerprints retained.

Clause 9 – Material retained for purposes of national security

14. Clause 9 allows for the retention of fingerprints and DNA profiles outside the prescribed periods where a senior police officer makes a determination in writing that retention is necessary 'for the purposes of national security'. Determinations last 2 years but are renewable. We note that these determinations are to be reviewed by the Commissioner for the Retention and Use of Biometric Material under clause 19, who has the power to order destruction of retained material where he or she is satisfied that it is not necessary. Although we welcome the introduction of safeguards against unnecessary retention on national security grounds, we reiterate our view that prior judicial authorisation is typically a better mechanism for dealing with these kinds of questions than the establishment of specialist Commissioners.

Clause 17 – Exclusions for certain regimes

15. Clause 17 exempts DNA profiles and fingerprints taken from persons arrested under section 41 of the Terrorism Act 2000 from the retention scheme provided by the Bill. Given that separate provision has already been made under clause 9 for retention of DNA profiles on national security grounds, we see no reason why terrorism offences should be treated differently than other violent offences, i.e. as qualifying offences under the retention regime.

Clause 20 – National Security: Appointment of a Commissioner

16. Clause 20 established the Commissioner for the Retention and Use of Biometric Material, who has a particular role to play in reviewing national security determinations for retention of material under a number of different schemes. Although we very much welcome this principled attempt to strengthen the safeguards against unnecessary retention and use of DNA material on national security grounds, we wonder whether - rather than adopting a system of determinations reviewed by a commissioner - these functions could not be carried out more effectively by instead requiring any application for extended retention on national security grounds to be authorised by a Crown Court judge. This would have the merit of incorporating effective judicial control of retention decisions, while preventing the unnecessary proliferation of oversight mechanisms.

Clauses 26-28 – Protection of Biometric Information of Children in Schools etc.

17. The Coalition programme for government promised to 'outlaw the fingerprinting of children at school without parental permission'.[7] Clauses 26 to 28 implement this promise, by preventing the processing of a child's biometric data without the consent of both parents.

18. JUSTICE welcomes this measure. As the explanatory notes make clear, a number of schools have in recent years adopted biometric recognition systems 'for a variety of purposes including controlling access to school buildings, monitoring attendance, recording the borrowing of library books and cashless catering'. In our view, the routine gathering of students' biometric data for the sake of administering school lunches and library borrowing exemplifies a more general trend over the past decade, which is the wholly unnecessary and disproportionate gathering of sensitive personal biometric information for the sake of administrative convenience. It also demonstrates an inherent weakness in the current Data Protection regime for, as the Information Commissioner's Office has conceded, there is 'nothing explicit in the [Data Protection] Act to require schools to seek consent from all parents before implementing a fingerprinting application'.[8]

19. Indeed, as the law currently stands, we have serious doubts about the lawfulness of schools taking biometric data from students without consent and using it for purely administrative purposes. First, it is clear that the taking of biometric data engages a student's right to private life under article 8 of the European Convention, yet is unclear what lawful authority schools enjoy to take biometric information from students, nor the legitimate aim that schools are pursuing in doing so. In addition, article 16(1) of the of the UN Convention on the Rights of the Child ('CRC') provides that:[9]

> No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.

20. However, even if schools were found to enjoy sufficient authority under existing legislation to obtain students' fingerprints, we consider that the collection of such material is likely to be held a disproportionate measure under Article 8(2). As the House of Lords concluded in its judgment in *Huang and Kashmiri v Secretary of State for the Home Department* [2007] UKHL 11, the principle of proportionality under Article 8(2) requires, among other things, the public authority to show that 'the means used to impair the right or freedom are no more than is

---

[7] See n1 above, p11.

[8] Information Commissioner's Office, 'The Use of Biometrics in Schools', August 2008.

[9] The UK ratified the CRC in 1991 but it has not been incorporated into UK law.

necessary to accomplish the objective' (para 19). In our view, the collection of fingerprint data from students for the sake of monitoring attendance, or regulating access to school meals and library books, plainly fails this basic test of proportionality. Although some kind of identification scheme may be a legitimate restriction on student privacy for the sake of these goals, schools are not permitted to gather highly personal data from students for this sake where a less restrictive (and almost certainly equally effective) means is available. It is obvious that an ordinary student card scheme, using photo ID, would be both equally effective and far less intrusive to student privacy than the use of fingerprint data from students. In the circumstances, we have no difficulty concluding that schools' collection of biometric data for these purposes is an intrusive and patently unnecessary measure.

Clauses 29-36 – Regulation of CCTV and other surveillance camera technology

21. It should be obvious to any reasonable person that the unregulated use of surveillance cameras – whether by a public authority, private company or ordinary individual - poses a serious threat to personal privacy in the UK. As long ago as 1970, we warned that rapid and ever-increasing pace of technological developments in the field of surveillance meant that the existing legal framework for the protection of privacy was inadequate:[10]

> *English law does … provide a remedy for some kinds of intrusion into privacy, but it is certainly not adequate to meet the activities of a society which is perfecting more and more sophisticated techniques for intrusion.*

22. Over forty years later, there are more CCTV cameras in the UK than any other nation on earth.[11] For instance, the London borough of Wandsworth operates 1113 CCTV cameras for a population of 260,380 people – the same number as those operated by the police in Boston (population 4 million), Dublin (population 1 million), Johannesburg (population 3 million) and Sydney (population 4.5 million) combined.[12] Shetlands Borough Council (population 22,000) has more CCTV cameras than the San Francisco Police Department (population 3 million).[13]

23. This unprecedented growth in public surveillance demonstrates that effective regulation of CCTV cameras in Britain is long overdue. Although the Data Protection Act governs certain aspects of CCTV usage (specifically the handling of sensitive personal data), it does not provide – and was never intended to provide – a comprehensive legal framework governing CCTV placement and usage. Similarly, the use of covert surveillance cameras by public

---

[10] *Privacy and the Law* (JUSTICE, 1970), para 85.

[11] BBC News, 'The statistics of CCTV', 20 July 2009.

[12] BBC News, 'Police 'not using CCTV properly'', 20 July 2009.

[13] Ibid.

authorities is governed by a Code of Practice under section 71 of the Regulation of Investigatory Powers Act 2000 but this does nothing to regulate their non-covert use, nor the everyday use of CCTV by private companies and individuals.

24. In 2003, for instance, the European Court of Human Rights found that the lack of any legal remedy for a Mr Peck whose failed suicide attempt was captured on CCTV and then distributed to the media by the local authority meant that the UK breached his right to privacy under article 8 ECHR. In another privacy case in 2004, Lord Hoffmann rejected the argument that this required the courts to develop a tort of invasion of privacy:[14]

> Counsel for the Wainwrights relied upon Peck's case as demonstrating the need for a general tort of invasion of privacy. *But in my opinion it shows no more than the need, in English law, for a system of control of the use of film from CCTV cameras which shows greater sensitivity to the feelings of people who happen to have been caught by the lens*.

25. Clauses 29 to 36 implement the Coalition government's 2010 promise to 'further regulate CCTV'.[15] In particular, Clause 29 requires the Secretary of State to prepare a code of practice governing the use of surveillance cameras, otherwise known as CCTV cameras.[16] It sets out certain broad areas that the code must address (e.g. the development or use of CCTV (clause 29(2)(a)), and others that it may address (including access to, or disclosure of, information obtained via CCTV (clause 29(3)(h)). However, the code need not be comprehensive (i.e. it 'need not contain provision about every type of surveillance camera system' (clause 29(4)(a)). We are not aware that any draft code has yet been published so it is accordingly impossible at the current time to assess the likely impact of its provisions.

26. It is, at any rate, unclear whether the code will extend to the use of CCTV by private companies and individuals, which account for a substantial number of CCTV cameras in the UK. Public authorities are at least required to comply with article 8 of the European Convention,[17] and will be required to have regard to the code when carrying out their functions (clause 33(1)). The strength of this requirement remains uncertain, though: courts will be able to 'take account' of any failure by a public authority to have regard to the code when

---

[14] *Wainwright v Secretary of State for the Home Department* (2004) 2 AC 406, para 33. Emphasis added.

[15] See n1 above, p11.

[16] We use the term CCTV generically. As the Royal Academy of Engineering noted in 2007, 'the term CCTV is now for the most part a misleading label. Modern surveillance systems are no longer 'closed-circuit', and increasing numbers of surveillance systems use networked, digital cameras rather than CCTV. The continued use of the term is an indicator of a general lack of awareness of the nature of contemporary surveillance, and disguises the kinds of purposes, dangers and possibilities of current technologies' (*Dilemmas of Privacy and Surveillance: Challenges of Technological Change* (March 2007), p33).

[17] See section 6 of the Human Rights Act 1998.

'determining any question' in civil or criminal proceedings (clause 33(3). However, clause 33(2) also provides that:

> A failure on the part of any person to act in accordance with any provision of the surveillance camera code does not of itself make that person liable to criminal or civil proceedings.

27. In addition, clause 34 requires the establishment of a Surveillance Camera Commissioner to review the operation of the Code and encourage compliance with it. As with the establishment of the Commissioner for the Retention and Use of Biometric Material, any move to strengthen independent oversight of CCTV usage is something to be encouraged. However, we question whether the creation of yet another Commissioner in the field of surveillance and data-gathering is necessarily the best way to provide this oversight. Plainly, the extent of CCTV usage in the UK is significant and therefore oversight will inevitably require a certain level of resources. But the existing oversight framework of surveillance under the Regulation of Investigatory Powers Act is already highly fragmentary and lacking in coherence. We strongly doubt that further fragmentation of oversight arrangements is desirable. Although we can see the case for a Surveillance Camera Commissioner to be appointed as an interim step, we believe that the most effective way forward in the medium and long-term is for the establishment of a more coherent scheme of independent authorisation and oversight of surveillance as part of a comprehensive overhaul of RIPA itself.

28. In conclusion, although we welcome the Coalition government's move to further regulate the use of CCTV, in the absence of a draft code it remains very much open to question whether the clauses will deliver the stringent regulation of CCTV that is so plainly needed in order to check the growth of public surveillance.

Clauses 37-38 – Safeguards for certain surveillance under RIPA

29. The use of surveillance powers by local authorities was the subject of consultation by the previous government and was reviewed by the Coalition government as part of its review of counter-terrorism powers. JUSTICE responded to the consultation in July 2009 and gave evidence to the counter-terrorism review in August 2010. We argued that there was no justification for local authorities to employ directed surveillance powers under the Regulation of Investigatory Powers Act 2000 ('RIPA') and recommended, more generally, that public authorities should only be empowered to use directed surveillance, employ covert intelligence sources or access communications data where they are involved in the investigation and prosecution of serious criminal activity, and that such powers should only be exercised with prior judicial authorisation.

30. The government's counter-terrorism review concluded that:[18]

> Magistrate's approval should be required for local authority use of all three techniques [directed surveillance, access to communications data and use of covert human intelligence sources] and should be in addition to the authorisation needed now from a local authority senior manager (at least Director level) and the more general oversight by elected councillors; and
>
> Use of RIPA to authorise directed surveillance only should be confined to cases where the offence under investigation carries a maximum custodial sentence of 6 months or more. But because of the importance of directed surveillance in corroborating investigations into underage sales of alcohol and tobacco, the Government should not seek to apply the threshold in these cases. The threshold should not be applied to the two other techniques (CD and CHIS) because of their more limited use and importance in specific types of investigation which do not attract a custodial sentence.

31. In his parallel report, Lord Macdonald of River Glaven QC, the former Director of Public Prosecutions, agreed with the Review's conclusions on this issue.[19]

32. Accordingly, clauses 37 and 38 prevent an authorisation for directed surveillance, access to communications data or use of a covert human intelligence source from taking effect unless and until it has been approved by a magistrate. In particular, proposed clauses 23A(4) and 32A(3)(a) of the Regulation of Investigatory Powers Act 2000 direct that a magistrate may approve an authorisation 'if and only if' he or she is satisfied that 'there were reasonable grounds for believing' that the authorisation was properly made, and the relevant conditions were met – in particularly the necessity and proportionality requirements of subsections 28(2) (directed surveillance), 29(2) (covert human intelligence sources), and 22(1) and (5) (communications data).

33. We very much welcome the proposed introduction of prior judicial authorisation for local authorities using surveillance powers under RIPA. However, it raises the much more fundamental question of why prior judicial authorisation is not more widely used throughout RIPA. For instance, directed surveillance by police can be authorised by a police superintendent without judicial authorisation. Intrusive surveillance by police normally requires

---

[18] Home Office, *Review of Counter-Terrorism and Security Powers: Review Findings and Recommendations* (Cmnd 8004, January 2011) p27.

[19] *Review of Counter-Terrorism and Security Powers: A Report by Lord Macdonald of River Glaven QC* (Cmnd 8003, January 2011) pp6-7.

prior authorisation from a surveillance commissioner (a judicial office) but intrusive surveillance by the intelligence services is authorised by the Home Secretary. Similarly, interception of communications – arguably the most intrusive form of surveillance of all – is not subject to prior judicial authorisation but a warrant by the Home Secretary.[20] In JUSTICE's view, this patchwork of different authorisation schemes is inefficient and fails to provide sufficient safeguards against unnecessary and disproportionate use of surveillance powers.

34. We therefore propose that a far more principled, coherent and streamlined procedure would be to introduce prior judicial authorisation for interception of communications, all instances of intrusive surveillance, and all serious forms of directed surveillance. Whereas magistrates would be sufficient to authorise the use of surveillance powers by local authorities and other regulatory public bodies, security concerns could be dealt with by having the more serious forms of surveillance authorised by a Crown Court or a Divisional Court judge. We note that prior judicial authorisation of search warrants has been established practice for several centuries. Police are therefore already extremely familiar with the process of obtaining a warrant from a judge. We see no reason why the same procedure could not be adapted to require judges to issue surveillance warrants as well. As the European Court of Human Rights has held:[21]

> The rule of law implies, *inter alia*, that interference by the executive authorities with an individual's rights should be subject to effective supervision, which should normally be carried out by the judiciary, at least in the last resort, since judicial control affords the best guarantees of independence, impartiality and a proper procedure.

And, as the Court noted in a separate case:[22]

> It is, to say the least, astonishing that [the] task [of authorising interceptions] should be assigned to an official of the Post Office's legal department, who is a member of the executive, without supervision by an independent judge.

As with other kinds of oversight mechanisms, introducing prior judicial authorisation throughout RIPA would also reduce the need for the *ex post facto* independent oversight provided by the current Surveillance Commissioners, the Interception of Communications Commissioner and the Intelligence Services Commissioner.

---

[20] This does not include the various forms of interception that do not require a warrant under Part 1 of RIPA, (.e.g. monitoring of phone calls from prisons) none of which require judicial authorisation either.

[21] *Rotaru v Romania* (2000) 8 BHRC 43 at para 59.

[22] *Kopp v Switzerland* (1999) 27 EHRR 91 at para 74.

Clauses 39-53 – Protection of property from disproportionate enforcement action

35. Although the common law traditionally provided strong protection against entry and search of private property without the occupier's consent,[23] this has been greatly eroded over the years by a wide array of statutory powers. As the explanatory notes state, there are now 'around 1200 separate powers of entry contained in both primary and secondary legislation'. In JUSTICE's view, this number likely reflects the more general growth of coercive and intrusive powers granted to various public bodies for regulatory purposes – a trend analysed at length by the Law Commission in its recent consultation paper, *Criminal Liability in Regulatory Contexts*.[24]

36. Although we very much welcome the Bill's attempt to stem the tide of unnecessary legislation and curtail the growth of disproportionate search powers, we are concerned at the method adopted and question whether it might not be used to perversely expand the scope of search powers in current legislation.

37. Clauses 39 to 53 are effectively an extended series of Henry VIII clauses that enable ministers to repeal powers of entry and add safeguards but also to make 'modifications' (clause 40) and, in particular, to 'rewrite' powers of entry 'with or without modifications' (clause 41). We note that clause 41(3) seeks to limit the *vires* of the rewriting power to those situations where the changes in question 'provide a greater level of protection than any safeguards applicable immediately before the changes'. However, it is unclear how this assessment is to be made and, more importantly, who it is to be made by: the minister rewriting the provision, or the court assessing whether the rewriting was valid? As a rule we think it is constitutionally undesirable to rely on such broadly-worded provisions that enable the executive to rewrite laws enacted by Parliament, no matter how desirable the purpose may seem. We note also the recent warning given by the Lord Chief Justice, Lord Judge against reliance on such clauses:[25]

> You can be sure that when these Henry VIII clauses are introduced they will always be said to be necessary. But why are we allowing ourselves to get into the habit of Henry VIII clauses? Why should we? By allowing them become a habit, we are already in great danger of becoming indifferent to them, and to the fact that they are being enacted on our behalf. I do not regard the need for affirmative or negative resolutions as a sufficient protection against the increasing apparent indifference with which this legislation comes

---

[23] See e.g. *Seyman's Case,* 5 Co. Rep. 91a, 91b, 195 (KB 1603) per Coke LJ: 'the house of everyone is to him as his castle and fortress'.

[24] Consultation Paper 195.

[25] Lord Judge CJ, Mansion House Speech, 13 July 2010, p6.

into force. To the argument that a resolution is needed, my response is, wait until the need arises, and go to Parliament and get the legislation through, if you can. I continue to find the possibility, even the remote possibility, that the Treasury may by order disapply any rule of law, or a Minister may change our constitutional arrangements, to be rather alarming.

38. The Lord Chief Justice went on to express the hope that the Coalition government would seek to curtail their use:[26]

> When the Great Repeal Act is under consideration, I do urge that somehow, somewhere, Henry VIII clauses and indeed, the modern clause which in reality is Henry VIII Plus clauses should be excluded from the lexicon, unless the Minister coming to the House says in express and unequivocal language that he or she is seeking the consent of the House to such a clause.

39. In addition, we note that although clause 47 provides for a code of practice to provide guidance for the exercise of powers of entry, there is no reference whatsoever to Code B of the Police and Criminal Evidence Act 1984 which already governs search of premises, let alone any indication of how the code of practice would interact with the well-established provisions of the PACE Code.

40. In conclusion, we would urge the Coalition to seek a much more tightly-defined approach to the issue at hand. As with the provisions of the Public Bodies Bill, the better means of dealing with large amounts of unnecessary primary legislation is to take the time to repeal it in the proper manner, however long and unattractive the task, rather than granting the executive the extraordinary power to rewrite Parliament's laws.

Clause 57 – Permanent reduction of maximum period of detention to 14 days

41. JUSTICE has consistently opposed the various attempts to increase the maximum period of pre-charge detention that have been made since 9/11, including most recently the previous government's proposal to extend the maximum to 42 days in 2008. In our response to the Home Office review of counter-terrorism powers in August 2010, we argued that the *maximum* period of pre-charge detention under section 41 of the Terrorism Act 2000 be restored to its original limit of 7 days (although we do not rule out that even lesser periods of detention may breach article 5(4) ECHR). We also recommended that Schedule 8 of the 2000 Act be amended to ensure that all authorisation hearings are *inter partes* on the basis of evidence disclosed to the detainee.

---

[26] Ibid.

42. We therefore welcome the provision in clauses 57 to repeal the 28 day maximum established under the Terrorism Act 2000 as an important step in rolling back the disproportionate counter-terrorism measures of the past decade. Plainly, other steps still need to be taken. Nonetheless, the reduction to 14 days at least demonstrates a shift towards a UK counter-terrorism policy that is rational, evidence-based and governed by respect for fundamental rights.

Clauses 58-62 – Stop and search powers

43. In January 2010, the European Court of Human Rights in *Gillan and Quinton v United Kingdom* held that the stop and search power under section 44 breached the right to privacy under article 8 because of its lack of safeguards against arbitrariness.[27] In particular, it noted the 'breadth of the discretion conferred on the individual police officer' and the lack of any requirement on the senior police officer authorising the use of the stop and search power to make 'any assessment of the proportionality of the measure'.[28] Nor did the weak temporal and geographical limitations provided by sections 44(4) and 46(2) offer 'any real check on the authorising power of the executive'.[29] The availability of judicial review was also not an effective safeguard. As the Court noted:[30]

> in the absence of any obligation on the part of the officer to show a reasonable suspicion, it is likely to be difficult if not impossible to prove that the power was improperly exercised.

In light of the Court's ruling, the Coalition government directed police not to carry out pedestrian searches under section 44(2). It now seeks to implement the Court's ruling, repealing the previous stop-and-search scheme under sections 44 to 47 of the 2000 Act, (clause 58) and implementing a new scheme under 43B (inserted by clause 60).

44. In our submission to the Home Office review of counter-terrorism powers in August 2010, we made clear that we did not oppose the use of stop and search without reasonable suspicion in every circumstance. Indeed, it seemed to us that the original intention behind the section 44 power was a legitimate one: to enable blanket searches to be carried out in a specified area for a limited period where there was some real and immediate risk justifying the use of the power, e.g. a cordon around St Paul's Cathedral as a response to a bomb threat. As the Court

---

[27] (2010) EHRR 45.

[28] Paras 80-83.

[29] Ibid.

[30] Para 86.

held in *Gillan*, however, the safeguards in sections 44-46 proved wholly inadequate. We therefore recommended the following safeguards:

(a) raise the threshold for authorisations (e.g. no longer 'expedient' but based on a 'real and immediate risk');

(b) restrict significantly the duration and area of authorisations (e.g. lasting no more than 24 hours, not greater than 1 square mile, etc); and

(c) replace the current model of police authorisations with a system of prior judicial authorisation, preferably by way of *ex parte* application to a Crown Court judge (although there should remain provision for emergency authorisation by a senior police officer in circumstances where there is not sufficient time to apply to the court).

45. The Home Office review subsequently recommended 'significant changes' to 'bring the power into compliance with ECHR rights':[31]

> i. The test for authorisation should be where a senior police officer reasonably suspects that an act of terrorism will take place. An authorisation should only be made where the powers are considered "necessary", (rather than the current requirement of merely "expedient") to prevent such an act;
>
> ii. The maximum period of an authorisation should be reduced from the current maximum of 28 days to 14 days;
>
> iii. It should be made clear in primary legislation that the authorisation may only last for as long as is necessary and may only cover a geographical area as wide as necessary to address the threat. The duration of the authorisation and the extent of the police force area that is covered by it must be justified by the need to prevent a suspected act of terrorism;
>
> iv. The purposes for which the search may be conducted should be narrowed to looking for evidence that the individual is a terrorist or that the vehicle is being used for purposes of terrorism rather than for articles which may be used in connection with terrorism;

[31] *Review of Counter-Terrorism and Security Powers*, n18 above, p18.

v. The Secretary of State should be able to narrow the geographical extent of the authorisation (as well being able to shorten the period or to cancel or refuse to confirm it as at present); and

vi. Robust statutory guidance on the use of the powers should be developed to circumscribe further the discretion available to the police and to provide further safeguards on the use of the power.

46. The proposed power to conduct searches of pedestrians and vehicles under clause 43B is broadly similar in its outline to that under section 44, but has been more tightly drawn. Consistent with the recommendations of the Home Office's Counter-Terrorism Review, authorisation requires a senior police officer to both 'reasonably suspect that an act of terrorism will take place' *and* that 'the authorisation is necessary to prevent the act' In addition, the area authorised must be 'no greater than is necessary to prevent such an act' and the duration must similarly be 'no longer than is necessary' (clause 43B(1)). These requirements of necessity and proportionality are significant improvements over the previous section 44 power in terms of its compatibility with article 8 ECHR. The purposes for which searches may be carried out has also been slightly narrowed, consistent with the Review's recommendation.

47. Paragraph 6 of Schedule 5 further limits the maximum period for an authorisation under clause 43B to 14 days. Authorisations must also be confirmed by the Secretary of State within 48 hours of their making or lapse (paragraph 7(2) of schedule 5). Both the Secretary of State or another senior police officer may make further restrictions on the time and scope of an authorisation (paragraphs 7(4) and 9). As recommended, clause 61 also requires the Secretary of State to establish a Code of Practice concerning the exercise of the stop and search powers under sections 43 to 43B.

48. However, although JUSTICE considers that the safeguards in clause 43B represent a genuine improvement over those in section 44, they are not in themselves enough to ensure its compatibility with article 8 ECHR. In particular, it is important to note that the Court in *Gillan and Quinton* expressed grave concerns about 'the breadth of the discretion conferred on the individual police officer',[32] which gave rise to 'a clear risk of arbitrariness in the grant of such a broad discretion to the police officer'.[33] It concluded that 'in the absence of any obligation on the part of the officer to show a reasonable suspicion, it is likely to be difficult if not impossible to prove that the power was improperly exercised'.[34] Since clause 43B does not impose any requirement for the officer exercising search powers to have reasonable suspicion (clause

[32] Para 83.

[33] Para 85.

[34] Para 86.

43B(5)), it is all the more important for these risks of arbitrariness to be offset by safeguards that restrict its use only to circumstances where it is necessary and proportionate. In other words, the less constraints there are upon the discretion of the individual police officer exercising search powers, the more important the need for stringent checks on the ability to authorise such searches.

49. As it is, although the authorisation process in clause 43B has been improved, judicial review remains the only means by which the police authorisation can be challenged. However, the Court in *Gillan* expressed serious concern at the adequacy of judicial review:[35]

> Although the exercise of the powers of authorisation and confirmation is subject to judicial review, the width of the statutory powers is such that applicants face formidable obstacles in showing that any authorisation and confirmation are *ultra vires* or an abuse of power

Moreover, although the exercise of stop and search powers was subject to the more general oversight of the independent reviewer of terrorism legislation, the Court noted that the independent reviewer had 'no right to cancel or alter authorisations'.[36] For JUSTICE, this demonstrates the importance of having police authorisations subject to independent and impartial review *before* stop and search powers are exercised.

50. We therefore recommend that clause 43B be amended to require police authorisations to be approved by a Crown Court judge. Just as the police are normally required to seek a warrant from a judge before conducting a search of private premises, the police should be required to seek judicial approval before authorising the use of stop and search powers without reasonable suspicion within a particular area for a particular time. In those cases where there is not sufficient time for police to apply *ex parte* to a judge for approval, we recommend that police have the power to make emergency authorisations without prior judicial approval, but that such authorisations must be confirmed by a judge within 48 hours. We note that this is very similar to the model provided by paragraph 7(2) of Schedule 5 as currently drafted, under which any authorisation by police must be confirmed by the Secretary of State within 48 hours or lapse. Given that the Coalition government has already accepted the desirability of having police authorisations confirmed by a separate body, we think the case for that confirmation being made by a judge rather than a government minister is overwhelming.

---

[35] Para 80.

[36] Para 82.

Part 5 – Safeguarding vulnerable groups, criminal records, etc

51. Part 5 introduces a series of measures aimed at reforming the Vetting and Barring regime, and makes provision for disregarding criminal convictions for consensual gay sex between adults under the old Sexual Offences Act 1956. We welcome these reforms. Among other things, it is evident that the scope of the Vetting and Barring regime – while undoubtedly created to serve an extremely important function of public protection- was unduly rigid in its operation, imposed a disproportionate burden on those whose activities involved contact with vulnerable persons, posed further obstacles to the rehabilitation of persons who had criminal convictions for often minor offences, and raised particular concerns about the use and accuracy of so-called 'soft' information gathered by police and other authorities. The case for disregarding the convictions of persons convicted of buggery where the criminal activity in question was consensual sex between adults is even more inarguable.

Clauses 92-98 – Freedom of Information and Data Protection

52. In its programme for government, the Coalition promised to 'extend the scope of the Freedom of Information Act to provide greater transparency' and to 'create a new 'right to data' so that government-held datasets can be requested and used by the public, and then published on a regular basis'.[37] In our response to the Coalition's programme, we welcomed this announcement on the basis that the right to access government data is an important complement to the principles of freedom of information, and the right to receive and impart information under Article 10 ECHR. More generally, it promotes democratic transparency and accountability, and more effective public policy. We therefore welcome the measures adopted in clauses 92 to 98.

Clause 99 – Repeal of provisions for conducting certain fraud cases without jury

53. In its programme for government, the Coalition also promised to 'protect historic freedoms through the defence of trial by jury'. Clause 99 of the Bill would repeal the provision made in the Criminal Justice Act 2003 for the prosecution to seek to try cases of serious fraud without a jury.

54. JUSTICE has consistently opposed measures to restrict the right to trial by jury, both in cases of serious fraud (section 43 of the 2003 Act) and where there are concerns about jury tampering (section 44 of the same Act). In particular, the power under section 43 has never been brought into force, despite an attempt by the previous government to do so in 2005. The measure had been justified by the government by reference to the complexity of serious fraud

[37] N1 above, p21.

trials and the concern that lengthy trials may collapse due to a lack of understanding on the part of jurors. However, the government gave no evidence to support its claim and, indeed, contradicted evidence from the courts themselves. As the trial judge told the jury at the end of the ten-month long *Wickes* fraud case:[38]

> Those who may hereafter criticise juries' appreciation of lengthy and complex fraud cases would have done well to see the care and attention that … you have given to the case throughout.

Similarly, a juror in the Jubilee Line case commented to the media that there was no difficulty with the jury understanding the evidence.[39] Juries were, in effect, being blamed for the failings of the prosecution and poor case management by the courts themselves.

55. As we argued in opposing the introduction of these measures, jury trial is a constitutional right and deserves corresponding protection in UK law. The best protection is, of course, the restraint of Parliament in not enacting legislation that would abridge it. We therefore strongly welcome the proposed repeal of section 43 and urge that consideration be given to the repeal of section 44 as well.

ERIC METCALFE
Director of Human Rights Policy
JUSTICE
25 February 2011

---

[38] *R v Sweetbaum and others*, unreported, 25 November 2002

[39] David Leigh writing in the *Guardian*, March 24, 2005