Investigatory Powers Bill, the Prevent duty, state secrecy and fundamental rights

- Adam Straw -

1. In the 15 or so minutes I have available, I am going to try to talk about three pretty complicated topics.

(1) The Investigatory Powers Bill

2. On 11 October 2016 the IPB passed the report stage, which leaves only the third reading before royal assent. It is likely to become law in January 2017.

3. The Bill is an unprecedented legislative assault on privacy. Although it is welcome in that it seeks to regulate what the authorities have been doing anyway without any formal legal basis, it contains incredibly far-reaching powers with insufficient oversight.

The law

4. The IPB's current incarnation[1] is 261 pages long. It is accompanied by separate explanatory notes[2], and 6 draft Codes of Practice[3] which together run to over 400 pages. If you would like help deciphering the Bill and understanding some of its problems, have a look at the excellent posts on the Privacy International and Liberty websites.

5. There is a great deal of caselaw that is relevant. For example, the ECtHR Grand Chamber decision of *Zakharov v. Russia* [2016] 39 BHRC 435 reads like a manual for legislation governing the interception of communications. It identifies many particular requirements within article 8, and a number of specific flaws with the Russian legislation.

---

[1] www.publications.parliament.uk/pa/bills/lbill/2016-2017/0062/17062.pdf
[2] www.publications.parliament.uk/pa/bills/lbill/2016-2017/0040/17040en.pdf
[3] www.gov.uk/government/publications/investigatory-powers-bill-codes-of-practice

6. There are also important common law and EU Law cases. The latter include *Digital Rights Ireland* [2015] QB 127 and *Schrems v. Data Protection Commissioner* C-362/14. The implications of *Digital Rights Ireland* are due to be clarified by the ECJ shortly, in *Watson & Others* C-698/15, following a reference from the Court of Appeal in the case of *R (Davis) v. Secretary of State for the Home Department* [2015] EWCA Civ 1185, and so I will not analyse that case in detail here. *Schrems* indicates that broadly similar requirements to those described in *Zakharov* are contained within EU Law. However as the status of EU law is unclear, I will concentrate here on the ECHR.

Is there anything unlawful in the Bill?

7. There are a number of aspects of the Bill which appear either to be unlawful, or which will need to be clarified by legal action in the courts. A few examples are as follows.

i. Bulk warrants

8. Of particular concern are the bulk warrants in Parts 6 and 7 of the Bill:

   a. **A bulk interception warrant** authorizes or requires the interception of overseas communications in bulk: part 6, chapter 1.

   b. **A bulk acquisition warrant** permits the government to collect in bulk any communications data 'relating to the acts or intentions of persons outside the British Islands': part 6, chapter 2.

   c. **A bulk equipment interference warrant** allows the government to hack equipment to obtain bulk communications by, or information about, people overseas. They can use "any conduct… necessary" to achieve this aim. They may turn on a mobile phone's camera and microphone to see and hear what you are doing, or may alter or destroy the information on your computer: part 6, chapter 3.

d. **Bulk personal dataset warrants** enable the intelligence service to obtain a set of *any* personal data as defined by s.1(1) of the DPA 1998[4] relating to an unlimited number of people. It appears this extends not just to data held by the state but also by private organisations. The warrant may either be for a specific BPD or a class of BPDs: Part 7.

9. These are widely regarded as being extremely broad and intrusive powers. They will create large databases within government, and abroad, of the most sensitive information about the public at large. It is already clear that even the most secure database is open to being hacked and data being published or sold[5]; and that state agents are human and some will misuse the powers of secret surveillance[6].

10. The Bill only requires that the bulk warrants listed above are necessary and proportionate to the need to protect national security or prevent crime *in general terms.* There is no requirement for the intrusion be proportionate on the facts of an individual case.

11. For hundreds of years, the common law has prevented the use of "general warrants" which allow search and seizure in respect of classes of people, rather than specified individuals: e.g. *Leach v Money* IXXX St Tr 1021, at 1027. Lord Widgery CJ in *Williams v. Summerfield* [1972] 2 QB 512, at 519 observed:

> "generations of justices have, or I would hope have, been brought up to recognise that the issue of a search warrant is a very serious interference with the liberty of the subject, and a step which would only be taken after the most mature careful consideration of the facts of the case."

12. Many people's most sensitive personal information is contained or seen by their phones and computers. Having a phone or computer hacked is at least

[4] But also extending also to dead people.
[5] A few recent examples are the disclosure of the personal medical records of British sportspeople, and the sale of 500million records of Yahoo users.
[6] For example, the Ellison revelations of wrongful undercover policing in the Stephen Lawrence case, and the unlawful monitoring of legally privileged information in the Belhaj case. See also the Advocate General's opinion in C203/15 and C698/15, *Watson & Ors*.

as much an intrusion for many as having their home searched. It is certainly arguable that a hacking warrant is equivalent to a search warrant, and that the bulk provisions are contrary to those long-established principles.

13. Recent caselaw about whether the law governing the retention and disclosure of data by the police is contrary to article 8 is also relevant. For example, *R (T) v. Chief Constable of Greater Manchester* [2015] AC 49 concluded that there must be adequate safeguards in place to enable the proportionality of any interference to be adequately examined. Similarly, Strasbourg caselaw makes clear that the scope of any discretion conferred on the authorities must be clearly and precisely defined, to give the individual adequate protection against arbitrary interference[7].

14. A bulk warrant appears contrary to those principles. It defines the discretion in extremely broad terms, and does not require there to be any examination of individual cases where there may be compelling reasons why a warrant should not be granted.

15. The highly intrusive and widespread nature of the powers means compelling justification for them is necessary. It is for the state to prove that blanket powers of this nature are justified (*R (JF) v. Secretary of State* [2011] 1 AC 331). It is at least arguable that the state has not put forward sufficiently compelling evidence to discharge that burden. For example, it there appear to be less onerous measures which could do as much to achieve the aims pursued.

16. ECHR caselaw on secret surveillance shows even more clearly that the Act is likely to be contrary to article 8. For example, The Grand Chamber in *Zakharov* said the review of an authorisation:

> "260… must be capable of verifying the existence of a reasonable suspicion against the person concerned, in particular, whether there are

[7] For example, *Association for European Integration and Human Rights v. Bulgaria* Appn No. 62540/00, 28 June 2007 at §75, and *Weber v. Germany* [2008] 46 EHRR SE5 at §§93-94.

> factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures, such as, for example, acts endangering national security."
>
> "264… as regards the content of the interception authorisation, it must clearly identify a specific person to be placed under surveillance or a single set of premises as the premises in respect of which the authorisation is ordered."

17. Bulk warrants may be granted where there is no reasonable suspicion against anyone, and where the person or premises placed under surveillance will not be identified.

18. Albeit less problematic than bulk powers, the provisions regarding targeted surveillance appear to be unacceptable in article 8 terms. They enable thematic warrants to cover "a group of persons who share a common purpose", or "more than one person" where the warrant is "for the purpose of a single investigation" by the state. That means warrants can be issued which do not clearly identify a specific person to be placed under surveillance. This is a particular concern when the statutory provisions do not require there to be reasonable suspicion against anyone.

ii. Judicial Commissioners

19. Clause 23 states:

> "In deciding whether to approve a person's decision to issue a warrant under this Chapter, a Judicial Commissioner must review the person's conclusions as to… (a) whether the warrant is necessary… and … proportionate…
>
> In doing so, the Judicial Commissioner must (a) apply the same principles as would be applied by a court on an application for judicial review, and (b) consider [those] matters … with a sufficient degree of care to ensure that the Judicial Commissioner complies with the duties imposed by section 2…".

20. Clause 2 imposes general duties on public authorities, where the authority is making various key decisions under the Act. The duties are somewhat vague. They include that it may be necessary for the public authority to have regard to the Human Rights Act 1998.

21. *Zakharov* says this:

> "258. As regards the authority competent to authorise the surveillance, authorising of telephone tapping by a non-judicial authority may be compatible with the Convention… provided that that authority is sufficiently independent from the executive…
>
> 260. Turning now to the authorisation authority's scope of review... It must also ascertain whether the requested interception meets the requirement of "necessity in a democratic society", as provided by Article 8 § 2 of the Convention, including whether it is proportionate to the legitimate aims pursued, by verifying, for example whether it is possible to achieve the aims by less restrictive means…"

22. It appears that the only authority that will be able to satisfy this requirement in respect of interception and hacking warrants, is the Judicial Commissioner. The Home Secretary will not be able to do so, as she does not have the independence necessary: *Zakharov* at §258 and 278.

23. A key question is what standard of review must the Judicial Commissioner apply? This will determine whether the Judicial Commissioner is a safeguard with any substance. Where national security and foreign policy are concerned, the courts ordinarily leave a great deal of discretion to the executive. If that approach is applied in this context, that will plainly fail to comply with what *Zakharov* requires, which is that the JC must decide necessity and proportionality *for itself.*

24. At an early stage, to clarify this issue, it will be important for the Judicial Commissioner to disclose what standard of review it applies. The need to do so is supported by ECHR caselaw, which repeatedly recognizes that the legal framework must be made publicly available: see, for example, *Zakharov* at §276 and 283. In *Santare & Labaznikovs v. Latvia* appn no. 34148/07, 31 March 2016, the fact that the applicants could not verify that the judicial authorisation had applied appropriate principles, breached article 8. If the JC does not decide necessity and proportionality for itself, this could be challenged in the courts.

25. Other aspects of the procedure involving Judicial Commissioners may also need to be clarified. For example, it may be argued that in some cases it is necessary, to comply with principles of fairness in particularly sensitive applications, for special advocates to be appointed: *Al-Rawi v. Security Services* [2012] 1 AC 531, §173.

iii. Retrospective review?

26. Often, after the aims of an interception or hacking warrant have been achieved, there will be no reason not to tell the subject that a warrant had been granted. That would enable the subject to retrospectively review the decision to grant a warrant. Given that in general it will not be possible to enable the subject to review the decision in advance, retrospective review would be a crucial safeguard. It would be crucial in practical terms. The history of the IPT shows that in the absence of public scrutiny, it has not performed any significant role in checking the power of the executive. Until the case of *Liberty v. GCHQ* was decided in February 2015, the IPT had never once found against the government.

27. It is also arguably necessary in legal terms. *Zakharov* states:

> "287… As soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should, however, be provided to the persons concerned…"

28. This would then enable the target to apply for a review of the decision to grant the warrant, retrospectively. However, *Zakharov* continues:

> "288… By contrast, in the case of *Kennedy* the absence of a requirement to notify the subject of interception at any point in time was compatible with the Convention, because in the United Kingdom any person who suspected that his communications were being or had been intercepted could apply to the Investigatory Powers Tribunal, whose jurisdiction did not depend on notification to the interception subject that there had been an interception of his or her communications (see *Kennedy*, cited above, § 167)."

29. The power to apply to the IPT (which comes from s.65 RIPA 2000) will continue in respect of many of the powers within the IPB. It is arguable that *Kennedy* should be departed from insofar as the IPB is concerned. The

new Bill contains different and considerably more intrusive powers than those that were at issue in *Kennedy*. Caselaw has moved on since then, and s.65 RIPA is due to be amended. It is possible that the courts will decide that, in appropriate cases, a claimant should be notified that a warrant was granted, and the reasons for that grant, so that the subject may have a right of retrospective review.

iv. Metadata

30. Parts 3 and 4 govern the obtaining and retention of "communications data". This is sometimes referred to as metadata. It is defined in very complex terms (e.g. cl.237), which broadly mean information that identifies or describes a communication, but does not include the content of it. It includes metadata about internet use: "internet connection records" (cl.59(7)).

31. The government claims that communications data is far less intrusive than the content of communications. The courts disagree, and have recognized that metadata can be even more revealing and intrusive than content data, especially when aggregated[8]. Under these provisions, the police will be able to look up every website you have visited in the last year. They won't need a warrant to do so, or any basis for suspicion that you have acted unlawfully.

32. Parts 3 and 4 of the IPB retain a similar regime to that under RIPA and DRIPA in respect of metadata, but one which is significantly expanded. Under Part 4, the Secretary of State may require the blanket retention of all communications data for the entire population for up to twelve months. A large number of public authorities can grant themselves access to communications data. The power to do so is not limited to specified individuals, and can be exercised on a wide range of grounds, including to protect public health, or to help collect charges. In most cases, judicial

[8] Digital Rights Ireland (C-293/12), §72-74; Watson & Ors, §259; and Seitlinger and Others (C-594/12).

authorization is not required, nor in general is institutionally independent authorization required.

33. It is arguable that the legal framework governing communications data – since it is potentially so intrusive – must comply with similar standards to those concerning the interception of communications that are set out in *Zakharov* and other cases. The metadata provisions plainly do not comply with those standards. For example, no individual or premises need be specified; there is no provision for judicial authorization or review of decisions to obtain metadata; and it cannot be said that the provisions permitting such a large range of officials to have access to very sensitive data in bulk for such a broad range of purposes can be said to be strictly proportionate and necessary.

v. Interception taking place in immigration detention

34. Clause 49 makes lawful the interception of communications in immigration detention facilities, in exercise of a power conferred by the rules that govern the operation of those institutions[9]. There are basic rules regulating interception in prisons (e.g. reg.35A Prison Rules 1999) and psychiatric hospitals (§34 of the High Security Psychiatric Services (Arrangements for Safety and Security) Directions 2013) but none have yet been made to govern immigration detention.

35. It appears possible that interception is occurring, and will take place, pursuant to more general provisions (as it has in other contexts[10]). An example is rule 39 of the Detention Centre Rules 2001/238, which contains a general requirement for security to be maintained in immigration detention centers.

[9] There is a similar power in s.4 of the Regulation of Investigatory Powers Act 2000, regarding prisons and psychiatric hospitals. See also Prison Service Instruction 04/2016.

[10] See, for example, https://privacyinternational.org/sites/default/files/1.%20Claimant%27s%20Skeleton%20Argument.pdf.

36. If so, the absence of regulation for interception is likely to be unlawful. It may be possible to obtain further information as whether interception is currently occurring, for example by FOI requests. If rules are produced, they will need to contain detailed safeguards, for example as to the interception of communications between a detainee and her lawyer.

What legal challenges might be made, and how?

37. Leaving aside EU law, a claim might be made that the operation of certain provisions of the IPB is incompatible with article 8, or must be read and given effect in a way which is compatible with that article. Domestic law may be used to a similar end. For example, the principle of legality (by which statutory provisions must be read consistently with constitutional rights, unless it is clear Parliament intended they should not be) may be used to argue that parts of the IPB should be given a restricted interpretation.

38. How can a legal challenge be made? There is a general prohibition on disclosure in connection with legal proceedings of anything which suggests "interception-related conduct" has occurred (cl.53), subject to the exceptions in sch.3. This is one reason why taking legal proceedings to challenge the application of the IPB will be difficult. The IPB amends s.65 of RIPA, which sets out the circumstances in which a claim must or may be brought in the IPT. The decision about whether the claim should be brought in the IPT or by way of judicial review is a difficult one, which depends on factors such as the extent to which you rely on ECHR law, and whether you seek a declaration of incompatibility.

39. A person who is potentially at risk of being subject to surveillance can challenge the provisions of the IPB in the abstract. For example, in *Kennedy v. United Kingdom* [2011] 52 EHRR 4 an applicant was permitted to complain that the legislation was unlawful and incompatible with article 8, where "it could not be excluded that secret surveillance

measures were applied to him or that he was potentially at risk of being subjected to such measures."

40. However, it is best to obtain evidence to show that there is a basis for the belief that the claimant was subjected to surveillance. That is the test that was applied by the IPT in *Human Rights Watch v. Foreign Secretary* unreported, 16 May 2016. Privacy International represented 663 parties who had filled out a standard form saying they believed they had been subject to surveillance and as such could complain to the IPT. Only 6 of them had put forward enough evidence to satisfy the hurdle. (The IPT also said it could not entertain human rights complaints of anyone based outside the UK).

41. Nevertheless, a comparatively broad range of people or organisations can probably qualify as claimants, if they provide enough evidence. It is better if you can find a challenger who for specific reasons is at greater risk of unlawful surveillance than ordinary members of the public. For example, the challenger has particularly sensitive communications, metadata or information, such as a journalist, lawyer or MP; or the challenger holds information about, or communicates with, those overseas, and this might be picked up by the bulk provisions in parts 6 and 7. The more evidence you have to show that accessing the challenger's communications or information may cause harm, the better. By the same token, the more clearly irrelevant the challenger's communication or information is to national security or serious crime, the better.

The Prevent Duty

42. The Prevent duty is set out in section 26 of the Counter-Terrorism and Security Act 2015 (the "2015 Act"): "(1) A specified authority must, in the exercise of its functions, have due regard to the need to prevent people from being drawn into terrorism." Schedule 6 contains a list of specified authorities, which include nurseries, schools, universities and NHS Trusts.

43. There is a considerable amount of guidance, including statutory[11] and other[12] guidance, about the application of the Prevent duty in various contexts.

44. The aims of the scheme are of course extremely important. It seeks to combat terrorism, and insofar as it leads to action that rationally helps achieve that aim, and is proportionate, it is to be welcomed. But as Senator McCarthy shows us, it is possible to go beyond those limits.

45. Unfortunately, it is clear that the new duty and related guidance have been applied in some very worrying ways[13], including:

a. There are local authority policies which require, automatically, school teachers to report to the police and others anyone they think might be at risk of radicalization[14]. National policy on schools says "appropriate action" should be taken in such cases.

b. "At risk of radicalization" is defined extremely broadly. For example, there are a number of local authority policies which indicate that the signs of a risk of radicalization include: "Appearing angry about government policies, especially foreign policy" (Camden)[15], and "discussion of international conflicts" (Lancashire)[16].

c. There are a number of examples of very young children being referred under the Prevent duty to other services, including to the police. For example, a 2 year old child in East London who has a diagnosed

[11] *Revised Prevent Duty Guidance for England and Wales (July 2015)* under s.29 of the 2015 Act
[12] Such as the Department for Education's *Keeping children safe in education* July 2015, and *The Prevent duty: Departmental advice for schools and childcare providers June 2015*
[13] www.preventwatch.org/cases/
[14] For example, Central Bedfordshire Safeguarding Children Board's guidance entitled *Safeguarding Individuals Against Radicalisation or Violent Extremism*
[15] www.cscb-new.co.uk/wp-content/uploads/2015/10/CSCB_Radicalisation_and_Extremism_Single_Pages.pdf.
[16] www.preventforschools.org/download/file/Channel%20leaflet%20Updated%2020141.pdf.

learning disability sang an Islamic song and said 'Allahu Akbar' spontaneously. He was apparently referred to social services[17]. Two brothers, aged 5 and 7, who were perceived by their school to be muslims, were referred by their teachers to the police on the basis that they had received toy guns as presents. A 4 year old was referred to a Channel panel[18] after he draw a picture of his father holding a cucumber.

d. When data as sensitive as this is processed in this way, there is an inherent risk of it being disclosed more widely, and a number of examples of that happening. For example, in Waltham Forrest, several 9 and 10 year old school children had been identified as being "at risk of radicalisation". The names of the children and the fact that they had been identified as such were accidentally released to the public [19].

e. If a person is referred to the police because they are believed by a teacher to be at risk of radicalisation, the police may well retain a record. It is likely to be difficult to challenge a decision to retain that type of record, since police will often be entitled to rely on the views of a professional in this sense. It will also often be difficult to challenge a decision by the police to disclose, in the future, to a potential employer or other body that the pupil was believed to be at risk of radicalisation.

f. Disclosure is liable to cause serious detriments to the subject, particularly for muslims or certain ethnic minorities, whether that means losing a job, being socially ostracised, or otherwise. "At risk of radicalisation" means supporting terrorism or associated extremist ideologies. There is a grave stigma that attaches to someone though to be an Islamic extremist or terrorist.

---

[17] www.irr.org.uk/wp-content/uploads/2016/01/IRR_Prevent_Submission.pdf.

[18] A multi-agency service aimed at addressing concerns of radicalisation, see ss.36-41 of the 2015 Act.

[19] www.independent.co.uk/news/education/education-news/greenleaf-primary-school-council-to-investigate-how-names-of-school-children-at-risk-of-a6754881.html.

g. Many public servants have complained that the Prevent duty undermines their ability to perform their functions. For example, the National Union of Teachers said that the scheme causes suspicion in the classroom and confusion in the staffroom[20]. UNISON expressed deep concern at the vagueness of the duty, widespread potential for discriminatory behaviour, and a breakdown in trust between public servants and service users[21]. There is considerable evidence that it inhibits what young children talk about in the classroom[22], and that it has been applied in a number of cases in a discriminatory manner[23].

h. Public authorities may be sanctioned for failure to comply with the Prevent duty.

46. There are a number of respects in which the application of the Prevent duty, and the associated guidance, may be unlawful. There isn't time within this talk to look at all of these, so I will just pick a couple of examples.

47. The application of the Prevent duty may be direct discrimination, contrary to s.13 of the Equality Act 2010. An example is a Muslim child referred to the police merely because he was given a toy gun. It will be difficult for a school to prove that a white or Christian child would have been referred to the police on this basis.

48. Insofar as guidance *requires* schools to take action or refer a child to the police who they judge may be at risk of radicalization, the guidance is

---

[20] www.theguardian.com/politics/2016/mar/28/teachers-nut-back-motion-calling-prevent-strategy-radicalisation-scrapped

[21] http://www.preventforfeandtraining.org.uk/sites/default/files/Prevent-Duty.pdf

[22] http://www.irr.org.uk/wp-content/uploads/2016/01/IRR_Prevent_Submission.pdf, p.5.

[23] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/461404/6_1256_EL_The_Terrorism_Act_Report_2015_FINAL_16_0915_WEB.pdf e.g. p78; and https://www.london.gov.uk/sites/default/files/preventing_extremism_in_london_evidence_pack.pdf.

likely to be contrary to article 8 ECHR and the common law. Referral to the police may interfere with article 8, particularly if the police retain a record that school staff had formed this view. It is arguable that this blanket approach is impermissible, and that there must be a legal or policy framework in place which requires school staff to assess the proportionality of any such interference: *R (T) v. Secretary of State* [2015] AC 49, §114 (on article 8), and *R v. A Local Authority in the Midlands, ex p LM* [2000] 1 FLR 612 (on the common law).

49. Similarly, a referral to the agencies, particularly the police, indicating that a student may be an extremist or terrorist, is a matter which has the potential to cause a serious detriment to that individual. In consequence, article 8 ECHR, and associated international instruments, arguably require there to be published safeguards in respect of such powers, which (i) make adequately clear the scope of the authority's power and the circumstances in which it will be used, (ii) ensure the education authority examines the proportionality of the interference, and (iii) ensure accuracy and confidentiality: *M.M. v, United Kingdom* Appn. No. 24029/07, 13 November 2012, at §§193, 195, 200 and 206[24]; and EU Data Protection Directive 2016/680, of 27 April 2016, preamble §33 and 50.

50. The guidance to schools arguably fails to meet those requirements, for example because it defines 'at risk of radicalisation' extremely broadly and with insufficient clarity; it does not adequately explain to teachers why a referral may interfere with the individual's article 8 rights, for example by setting out the potential consequences of referring a child to the police; and it contains no additional safeguards to ensure information remains confidential and accurate.

[24] It is "essential… to have clear, detailed rules governing the scope and application of measures; as well as minimum safeguards concerning, inter alia... procedures for preserving the integrity and confidentiality of data… "

51. There are statutory[25] and other duties to protect and enable the freedom of expression in schools and universities. It is arguable that the guidance regarding universities is unlawful as it gives rise to an unacceptable risk of decisions being made that are contrary to those duties.

52. The Extremism Analysis Unit of the Home Office has publicly identified those it has decided are extremists or hate speakers, such as Dr Salman Butt. This has occurred without the subject having any right of reply, which is arguably contrary to rules of natural justice.

Secrecy and fundamental rights

53. I have been asked to fit in to the short remaining time a few points about fundamental rights and secrecy.

54. As is well known, the right to a fair trial is protected by article 6 ECHR. There must be certain procedural safeguards in the determination of civil rights or obligations. Before such a determination can be made by a public authority that will have a serious impact on fundamental rights, such as on liberty (*Secretary of State for the Home Department v. F* [2010] 2 AC 269) or property (*Bank Mellat v. HM Treasury* [2016] 1 WLR 1187), it may be necessary for an irreducible minimum amount of information to be disclosed. The common law contains similar safeguards.

55. In claims of public interest immunity, the courts will often defer to a reasoned view of the executive, supported by evidence, that disclosure will harm an important public interest. The courts should be less willing to do so where the proceedings at issue concern fundamental rights. There have been several cases in Strasbourg indicating that decisions to withhold disclosure on the basis that it would harm national security or serious crime, were unlawful, such as *Nasr and Ghali v. Italy* (44883/09), 23

[25] Such as s.43 Education (No 2) Act 1986 and s.202 of the Education Reform Act 1988.

February 2016; *El-Masri v. FYR of Macedonia* [2013] 57 EHRR 25; and *McKerr v UK* (2002) 34 EHRR 20, §149-160.

56. The courts may also draw inferences that ECHR rights have been breached, from a failure by the state to disclose relevant information: *Husayn v. Poland* [2015] 60 EHRR 16, §§395, 415 and 429. A similar approach is taken under the common law: for example *Gulati v. MGN Ltd* [2016] FSR 12, §85-96.

Adam Straw
Doughty Street Chambers
5 October 2016