

Prepared by Guy Herbert, General Secretary of NO2ID

## 1. Summary

Buried among the numerous complicated and controversial provisions of this legislation is a single clause, clause 152 in the first draft of the Bill, which is a profound threat to privacy, liberty and the rule of law. It is enabling legislation that converts the Data Protection Act into a machine for massively increasing the dealing by government in information of all kinds. It is designed to allow ministers to use a fast-track regulatory procedure to sweep away data protection, human-rights considerations, confidentiality, legal privilege, and ultra vires when they would stand in the way of any use, acquisition or dissemination of information in pursuit of departmental policy.

The availability of broad data-sharing along these lines would be a profound change in the way the country is governed, potentially altering the function of almost all other legislation. It should not be introduced at all, but certainly not without proper public debate. There has been no such debate.

It would be a disaster if the “information sharing order” (ISO in what follows) were to be successfully smuggled through parliament in this manner.

## 2. The Bill and NO2ID

The Coroners and Justice Bill contains numerous potentially controversial measures, on most of which NO2ID, as a single-issue campaign group, can have no view. We are concerned about information sharing and privacy in general, and reserve our comments relating to other parts of the Bill where there may be privacy issues involved. This briefing focuses solely on Part 8 of the Bill, which amends the Data Protection Act 1998, and principally on the single clause that creates ISOs. As well as multiplying the powers of all ministers, Part 8 increases the powers of the Information Commissioner. We are not persuaded by this quid pro quo, for reasons explained in section 8 below.

This briefing consists of 9 pages: 9 numbered sections (3pp) of general comments and a 7-page annexe with detailed notes on the legislative drafting. We are happy to discuss any points in it further.

## 3. The background

Reading the notes provided by the Ministry of Justice to accompany the Bill without prior knowledge of the subject, one might gain the impression that the concept of the ISO somehow springs from the Walport-Thomas Review, when in fact that review was set up by the Ministry of Justice in order to re-present the idea of information sharing, which had become somewhat discredited after the HMRC data-disc scandal of November 2007. NO2ID has chronicled the move to ever more arbitrary information sharing powers, since we observed the Children Act 2004 expressly set aside all common-law and statute rules of confidentiality for what eventually became ContactPoint.

The developing philosophy of government by information management that we characterise as “the database state”, has become Whitehall orthodoxy without any systematic public debate, and the ISO should be regarded as the outcome of a desire to manage the citizen centrally as a single file, rather than permit separate relationships with separate organs of state, and of an impatience with mediating institutions such as parliament and the rule of law. In this view, information sharing is seen as one-sidedly good for everyone. This is set out very clearly in a series of official documents on “Transformational Government” (The key ones are exhibited here: <http://www.no2id.net/datasharing.php>).

The Information Sharing: Vision Statement issued by the then Department of Constitutional Affairs in September 2006 identified the main ‘barriers’ to information sharing as data protection, the Human Rights Act, common law confidentiality, and *vires*.

## 4. Objections to information sharing provisions in principle

We think that the “barriers” are not random obstacles. They are principles that have evolved in the courts and been captured in statute precisely because they protect things in human life that are worth protecting.

NO2ID set out its views on the principles of information sharing in its evidence to the Walport-Thomas Review. Repudiating the implicit bias of that review, we said:

“There are no intrinsic benefits of data-sharing (which is a name for a wide class of processes or acts, not a coherent thing), and we do not accept the implied trade-off between individual privacy and any generalised social benefit. While all social relationships depend on some form of communication of personal information, data-sharing is purely ancillary to the relationships and individual or collective enterprises it facilitates. ... NO2ID regards privacy and personal control of personal information as primary goods, interfering with which requires specific justification in each case.”

The Home Affairs Committee, in its report *A Surveillance Society? (Fifth Report of Session 2007-08)* said much the same thing in more diplomatic language:

"The Government should give an explicit undertaking to adhere to a principle of data minimisation and should resist a tendency to collect more personal information and establish larger databases. Any decision to create a major new database, to share information on databases, or to implement proposals for increased surveillance, should be based on a proven need." (p.7)

We suggest that “proven need” requires direct oversight and scrutiny on each occasion, and that the proper place for the proof of need for a change in the law of the land is parliament. It is not necessary to agree with NO2ID on any particular case to accept that proposition.

The idea of proper oversight and a proven case for extensions of the database state is mocked by the “Henry VIII” clause before the House. Ministers would be enabled to remake the law ad lib by regulation; and be subject only to the most flaccid test – whether sharing contributes to the expedient pursuit of departmental policy.

## **5. Objections to information sharing provisions in practice**

It is a truth that ‘Information is power’. Arbitrarily extended power is likely to be arbitrarily exercised, and there is little indication that ministers or departments have come to terms with the problems of handling, protecting or properly interpreting huge volumes of information. Every sharing power not only creates potentially oppressive direct use by the authorities (our of error, inadvertence or callousness, more likely than design – see our briefing on the Serious Crime Bill (now Act) for more detail:

<http://www.no2id.net/IDSchemes/NO2IDSeriousCrimeBillBriefingFEB2007.pdf> ), but also avenues for unauthorised access to information, and therefore identity theft, stalking, or other persecution of individuals. Most obvious to the public in the light of the November 2007 child benefit records disaster, large scale sharing inevitably means large scale loss. Far from helping the public, as it purports to, joined-up government creates new risks, large costs, and the projected gains in ‘efficiency’ can seldom be quantified.

At its mildest, information sharing is a recipe for an enormous growth in bureaucratic empires and concomitant IT costs. Even ignoring the costs to liberty and privacy it should be very closely monitored for the sake of the public purse.

## **6. Information sharing provisions: Objections to process**

The government’s presentation of the clause 152 provisions is deceptive and disreputable. It is nearly the final clause in a long Bill stuffed with potential controversy. A timetable might well prevent it being discussed in the Commons at all.

It introduces an entirely novel principle and does it in a single clause. Yet all the surrounding language and publicity is designed to minimise the consequences of what is being done. A series of “safeguards” are suggested to be in place. But, examined closely, they are no such thing.

It is noticeable that by making ISOs orders under the Data Protection Act, they will carry the misleading label of “Data Protection” every time they are applied. It is calculated to be deceptive in operation, too.

## **7. Information sharing provisions: Political objections**

Though ISOs are a major change to the way Britain is governed, there is no electoral mandate for them. No attempt has been made to make any argument for them from political principle. None of this has been cleared with the public.

There is reason to believe public opinion is overwhelmingly opposed. NO2ID asked through ICM in December:

Q. You may have heard that the government intends to collect information about citizens and store it on large computer systems which can then be used for a wide range of purposes. Do you think storing information and sharing it between different parts of government in this way is a... good/bad idea. – 65% said a bad or very bad idea.

The Sunday Times/YouGov asked more directly in the second week of January:

Q. The Government has announced new data-sharing laws to allow public bodies, including town halls, access to your personal data held by other government bodies. Ministers say this will reduce inefficiencies, while critics say it is in breach of data protection laws.

Do you think this proposal will or will not give the Government too much access to your personal data? – Will give too much power - 65%; Will not - 19%; Don't know - 17%

The public does not trust government with its personal information. When these proposals become known and understood, there will be anger at the way they have been pushed forward semi-secretly despite all the government's reassurances that more care is being taken after a series of data disasters.

## **8. Assessment notices and codes of practice**

The ISOs will be said to be offset by increases in the Information Commissioner's powers. But nothing in the new powers serves to restrain ISOs themselves. As noted below in the detailed analysis, the Commissioner has almost no say over the content of ISOs. The increased powers are little constraint on government departments doing what they want with information, because to the extent that the ISO or other statute disapplies them, then the principles of Data Protection simply will not. The need for minute compliance with the letter of Codes of Practice is unlikely to inhibit a public authority. And collectively the civil service has many more staff to generate ISOs than the Commissioner is ever likely to have to assess them.

Meanwhile there is just too much work for the Commissioner to do plausibly. Adding to powers is unlikely to make a significant difference when the ICO has limited resources in the first place and is responsible for handling complaints on behalf of the entire country. NO2ID believes that a change to data protection law that grants millions of individuals directly enforceable rights over information pertaining to them is more likely to change corporate and departmental behaviour, than granting punitive power to a limited number of ICO staff.

What is more, issuing guidelines and punishing data controllers for failing to follow them, likely misses the existing defects in the Data Protection Act (the European Commission suggests that it fails to implement as much as a third of the relevant directive correctly). It is irrelevant too to the more substantial problems for privacy and information security that are created by a cult of sharing. What is needed is careful, honest, reassessment of our problem, not window-dressing.

## **9. NO2ID's recommendations**

Information sharing, privacy and data security are all matters of great public concern and profound political importance in an information age. They ought to be openly debated and significant changes made only in the open. Hasty fixes driven by the convenience of officialdom are (even leaving aside all the points above) unlikely to produce anything good. While we could afford to ignore clauses 151, 153, and 154 did they appear by themselves – as so much legislative displacement activity - parliamentarians should demand that the matters covered by Part 8 of the Bill are dealt with openly, in separate, fully timetabled legislation, and should make it absolutely clear that they will not permit such a broad enabling power as the ISO at all. Clause 152 is so dangerous that no conceivable amendment makes it tolerable in a democratic society. It should be struck out.

Guy Herbert  
General Secretary, NO2ID  
Box 412, 19-21 Crawford Street  
LONDON  
W1H 1PJ

Office: 020 7793 4005  
Mobile: 07956 544 308  
Email: [general.secretary@no2id.net](mailto:general.secretary@no2id.net)

## Annexe - Detailed Commentary on Clause 152

I have taken the text from the Bill as introduced on 14<sup>th</sup> January 2009

<http://services.parliament.uk/bills/2008-09/coronersandjustice.html>

I have made some typographical changes for clarity: in particular the Bill text is an italic serif face, the operative part of the Bill in bold italic, and the insertions it makes into the Data Protection Act in normal weight. Commentary is in this sans-serif face. Throughout I use “ISO” for “information sharing order”.

## ***152 Information sharing***

### ***(1) After section 50 of the Data Protection Act 1998 (c. 29) insert—***

*“Part 5A*

#### *Information Sharing*

##### *50A Power to enable information sharing*

*(1) Subject to the following provisions of this Part, a designated authority may by order (an “information-sharing order”) enable any person to share information which consists of or includes personal data.*

“enable.” It needs to be questioned whether “enable” here can include or be backed by some measure of compulsion or coercion, or financial inducement. There is reason to suspect that even if an ISO cannot be drafted to require sharing (which is not clear), then enabling sharing will lead to coercion in practice. Public authorities are adept at making various forms of compliance, and in particular data-collection, a condition of licensing or approval within their competence. (For example, the imposition of Metropolitan Police “Form 696” on music venues using licensing laws.)

“any person” An ISO may apply to information in the control of anyone. It is not just for information supplied to public authorities for their official purposes, as most of the discussion surrounding broad data-sharing supposes.

“which consists of or includes personal data” Very important. Provided the specified information includes personal data an ISO may permit it to be shared. This goes beyond the normal scope of the Data Protection Act immediately. There is not in general a power or an entitlement to share information regardless of whether or not it includes personal data. Though personal data has the additional (not very strong) protections conferred by the Data Protection Act, information that is not personal data often is protected by confidentiality or contractual obligation, and public authorities have no power to use, disseminate or collect information of any kind without legal authority. If one agrees that ‘information is power’ then the latter stricture is fundamental to the rule of law. Most business information includes some personal data, so would be included.

### *(2) For the purposes of this Part—*

*“designated authority” means—*

- (a) an appropriate Minister,*
- (b) the Scottish Ministers,*
- (c) the Welsh Ministers, or*
- (d) a Northern Ireland department;*

*“appropriate Minister” means—*

- (a) the Secretary of State,*
- (b) the Treasury, or*
- (c) any other Minister in charge of a government department.*

### *(3) For the purposes of this Part a person shares information if the person—*

- (a) discloses the information by transmission, dissemination or otherwise making it available, or*
- (b) consults or uses the information for a purpose other than the purpose for which the information was obtained.*

“consults or uses” note the extension of the use of “sharing” beyond its ordinary meaning. This shows the core of official expediency in the clause. And it contrasts with the consumerist rationale usually provided for data-sharing

about citizens, exemplified by 'Tell Us Once'. The story is citizens want voluntarily provided personal details to be passed to all relevant departments, and therefore barriers to data-sharing must be removed. But if citizens do intend such sharing it is a simple matter to identify that as part of the purpose for which information is being provided. The repurposing provision indicates that the general case is information concerning unwilling and unknowing citizens, and

*(4) A designated authority may make an information-sharing order only if it is entitled to make the order by virtue of section 50C and it is satisfied—*

“only” – Here and elsewhere is likely to be promoted as the sign of a ‘safeguard’. Examination of the surrounding detail however shows any safeguarding function to be nugatory. Note here that it is only the authority that must be “satisfied”, so the following notional tests will only be failed if not formally considered or it would be totally unreasonable to deem them met.

*(a) that the sharing of information enabled by the order is necessary to secure a relevant policy objective,*

Save in the devolved governments, “a relevant policy objective” is not limited to the discharge of existing departmental functions conferred by parliament. It could be a purely political goal or the pursuit of departmental aggrandisement. Ministers could use ISOs to extend their power by regulation.

*(b) that the effect of the provision made by the order is proportionate to that policy objective,*  
Empty because proportionality to the objective is guaranteed by the preceding ‘necessity’ test.

*and*  
*(c) that the provision made by the order strikes a fair balance between the public interest and the interests of any person affected by it.*

There is an implicit utilitarian calculus here – note interests are being balanced not rights, so the (undefined) public interest is highly likely to be deemed to outweigh that of any finite group of individuals or corporations. This is quite different from the test of ‘proportionality’ set up in human rights legislation.

*(5) An information-sharing order must—*

- (a) specify the person, or class of persons, enabled to share the information;*
- (b) specify the purposes for which the information may be shared;*
- (c) specify the information, or describe the class of information, that may be shared.*

*(6) An information-sharing order may not enable any sharing of information which (in the absence of any provision made by the order) would be prohibited by Part 1 of the Regulation of Investigatory Powers Act 2000 (c. 23) (communications).*

Note that the Explanatory Notes (para.696) on this point are arguably incorrect. The subclause is capable of bearing two readings. It can be maintained that there is nothing in this subclause that prevents an ISO being used to enable or require the sharing of intercepted communications – provided it makes express provision to modify Part 1 of RIPA accordingly.

In any event, the fact of this purported exclusion emphasises that an ISO may be used to enable sharing (including acquisition) of communications data, or of the product of intrusive surveillance under RIPA. One consequence is that no primary legislation would be needed for the Home Office to create a super-database of all communications data, as has been widely reported as an objective of the Intercept Modernisation Programme. Another is that an ISO could alter the authorisation procedures for RIPA requests for communications data.

*(7) Nothing in this section (or any information-sharing order) is to be taken to prejudice any power or duty to share information which exists apart from this section.*

*50B Information-sharing orders: supplementary provision*

*(1) An information-sharing order may—*

- (a) confer powers on the person in respect of whom it is made;*
- (b) remove or modify any prohibition or restriction imposed (whether by virtue of an enactment or otherwise) on the sharing of the information by that person or on further or onward disclosure of the information;*

The parenthesis gives officialdom the capacity to override and exclude lack of capacity, common law rules of confidentiality, any agreement or other undertaking or privilege, human rights law or even specific statutory prohibition.

*(d) confer powers on any person to enable further or onward disclosure of the information;*

So it can also grant powers to have confidentiality (etc) waived in the future, even if not directly excluded in the ISO.

*(d) prohibit or restrict further or onward disclosure of the information;*

*(e) impose conditions on the sharing of information;*

Which could include for example secrecy as to the fact of sharing.

*(f) provide for a person to exercise a discretion in dealing with any matter;*

*(g) enable information to be shared by, or disclosed to, the designated authority;*

*(h) modify any enactment.*

*(2) An information-sharing order may provide for the creation of offences triable either way which are punishable—*

*(a) on conviction on indictment, by imprisonment for a term not exceeding the specified period or to a fine or to both;*

*(b) on summary conviction, by imprisonment for a term not exceeding the specified period or to a fine not exceeding the statutory maximum or to both.*

This is slightly mysterious. It is likely that it will be justified by reference to safeguarding shared information by punishing unauthorised disclosure. This is not a plausible mechanism for preventing leaks in systems designed to collect and propagate information. Query, whether an ISO could be drafted so as to compel sharing by making refusal an offence?

*(3) In subsection (2)(a) and (b) “specified period” means a period provide for by the order but the period must not exceed—*

*(a) in the case of summary conviction, 12 months (or, in Northern Ireland, 6 months), and*

*(b) in the case of conviction on indictment, 2 years.*

*(4) A designated authority making an information-sharing order must ensure that any specified period for England and Wales which, in the case of summary conviction, exceeds 6 months is to be read as a reference to 6 months so far as it relates to an offence committed before the commencement of section 282(1) of the Criminal Justice Act 2003 (increase in sentencing power of magistrates’ courts from 6 months to 12 months for certain offences triable either way).*

*50C Designated authority: entitlement to make an information-sharing order*

*(1) An appropriate Minister is entitled to make an information-sharing order only if the sharing of information enabled by the order is for the purposes of—*

*(a) in the case of the Secretary of State, any matter with which a department of the Secretary of State is concerned;*

*(b) in the case of the Treasury, any matter with which the Treasury is concerned;*

*(c) in the case of any other Minister in charge of a government department, any matter with which that department is concerned.*

Again, this is likely to be presented as an important restriction. In fact the whole clause 50C is about the partition of power not its restriction. Some government department is “concerned” with every aspect of life, and non-departmental bodies each have a tutelary department.

*(2) Where more than one appropriate Minister is entitled to make an information-sharing order by virtue of subsection (1), any one or more of the appropriate Ministers acting (in the case of more than one) jointly is entitled by virtue of this section to make the order.*

*(3) The Scottish Ministers are entitled to make an information-sharing order only if the sharing of information to which it relates consists of one or both of the following—*

*(a) the disclosure of information by a relevant Scottish body to another such body where the information was held by the first body in connection with its devolved Scottish functions and is disclosed to the second body for the purposes of its devolved Scottish functions;*

*(b) a relevant Scottish body consulting or using information which was obtained by it for the purposes of one or more of its devolved Scottish functions for the purposes of any of its other devolved Scottish functions.*

Scottish and (below) Welsh and Northern Irish authorities are restricted in the scope of the orders they may make by the scope of devolved powers and to sharing within and between the limited universes of devolved bodies within their purview. This only emphasises how unlimited are ISOs available to Whitehall ministers, they are by contrast not limited to taking information from or passing it to public bodies, and they may take information from devolved bodies too, without the approval of the devolved governments (see below), as long as it is in pursuit of some non-devolved policy objective.

*(4) The Welsh Ministers are entitled to make an information-sharing order only if the sharing of information to which it relates consists of one or both of the following—*

- (a) the disclosure of information by a relevant Welsh body to another such body where the information was held by the first body in connection with its devolved Welsh functions and is disclosed to the second body for the purposes of its devolved Welsh functions;*
- (b) a relevant Welsh body consulting or using information which was obtained by it for the purposes of one or more of its devolved Welsh functions for the purposes of any of its other devolved Welsh functions.*

*(5) A Northern Ireland department is entitled to make an information-sharing order only if the sharing of information enabled by the order is for the purposes of any matter with which that department is concerned and that sharing consists of one or both of the following—*

- (a) the disclosure of information by a relevant Northern Ireland body to another such body where the information was held by the first body in connection with its devolved Northern Ireland functions and is disclosed to the second body for the purposes of its devolved Northern Ireland functions;*
- (b) a relevant Northern Ireland body consulting or using information which was obtained by it for the purposes of one or more of its devolved Northern Ireland functions for the purposes of any of its other devolved Northern Ireland functions.*

*(6) Where more than one Northern Ireland department is entitled to make an information-sharing order by virtue of subsection (5), any one or more of those departments acting (in the case of more than one) jointly is entitled by virtue of this section to make the order.*

*(7) In subsections (3) to (5) any reference to the sharing of information enabled by the information-sharing order includes a reference to any further or onward disclosure of information enabled by the order by virtue of section 50B(1)(c).*

#### *50D Consultation and Commissioner's report on draft order*

*(1) This section applies where a designated authority proposes to make an information-sharing order.*

*(2) The designated authority must—*

- (a) issue a general invitation to make representations, in a manner likely in the authority's opinion to bring the invitation to the attention of as large a class of affected persons who may wish to make representations as is reasonably practicable, and*

Note: "in the authority's opinion", which need not be correct.

- (b) take account of any representations made.*

Implicitly there may be as little as 21 days to make such representations and deal with them. This is an implausibly short period of time for a genuine consultation. Fortunately the consultation is guaranteed fake, because the only way representations could be taken account of is in relation to the meaningless 'balance' exercise of 50A(4)(c). The authority must take your interests into account, not your views.

*(3) The designated authority must submit a copy of the draft order to the Commissioner.*

*(4) The Commissioner may, within the 21-day period, submit to the designated authority a report stating whether or not the Commissioner is satisfied of the matters in section 50A(4)(b) and (c).*

The 21-day limit imposes a massive new burden on a Commissioner who is already overstretched. (No regulatory impact assessment of Part 8 of the Bill appears on the MoJ website, in contrast to the other parts.) To judge from government documents such as the Service Transformation Agreement there is likely to be an indefinite demand

for information sharing powers, any of which is likely to be extremely complex in its implications, if they are fully discernable at all. Note, too, that the Commissioner may not comment on the key 'necessity' test, of which the authority is the sole judge.

*(5) The designated authority may not lay the draft order before Parliament in accordance with section 67 before—*

- (a) the Commissioner submits a report under subsection (4), or*
  - (b) the end of the 21-day period,*
- whichever first occurs.*

*(6) If the Commissioner submits a report under subsection (4) and the designated authority proceeds to lay the draft order before Parliament, the designated authority must at the same time lay a copy of the report before Parliament.*

Which is calculated to have precisely no effect unless worded very strongly. Neither the Commissioner nor Parliament has the power to amend an ISO. It is take it or leave it. It seems unlikely that Parliament will find time to reject any ISOs unless there is huge publicity surrounding it in its as little as 3 weeks in draft.

*(7) In this section references to “Parliament” are to be read—*

- (a) in the case of a proposal of the Scottish Ministers to make an information-sharing order, as references to the Scottish Parliament;*
- (b) in the case of a proposal of the Welsh Ministers to make an information-sharing order, as references to the National Assembly for Wales;*
- (c) in the case of a proposal of a Northern Ireland department to make an information-sharing order, as references to the Northern Ireland Assembly.*

*(8) In this section—*

*“affected persons” means persons likely to be affected by the proposed information-sharing order;*  
*“the 21-day period” means the period of 21 days beginning with the day on which the designated authority gives a copy of the draft order to the Commissioner.*

#### *50E Requirements for consent and further consultation*

Not a safeguard. This is not consultation of anyone affected by the sharing of information about them. 50E merely preserves the bureaucratic hierarchy by ensuring mandarins get each other's permission for working in each other's areas of responsibility.

*(1) An information-sharing order made by an appropriate Minister (other than an order made by the responsible Secretary of State alone or jointly with another appropriate Minister) may be made only with the consent of the responsible Secretary of State.*

*(2) A designated authority (other than an appropriate Minister) must consult the responsible Secretary of State before making an information-sharing order.*

*(3) An appropriate Minister must obtain the consent of the Scottish Ministers before making an information-sharing order which—*

- (a) authorises information to be shared by or disclosed to a relevant Scottish body in connection with any devolved Scottish function of the body, or*
- (b) modifies any provision made by or by virtue of an Act of the Scottish Parliament or any subordinate legislation made by the Scottish Ministers.*

*(4) An appropriate Minister must obtain the consent of the Welsh Ministers before making an information-sharing order which—*

- (a) authorises information to be shared by or disclosed to a relevant Welsh body in connection with any devolved Welsh function of the body, or*
- (b) modifies any provision made by or by virtue of a Measure or Act of the National Assembly for Wales or any subordinate legislation made by the Welsh Ministers (or by the National Assembly for*

*Wales established under the Government of Wales Act 1998).*

*(5) An appropriate Minister must obtain the consent of the appropriate Northern Ireland department before making an information-sharing order which—*

- (a) authorises information to be shared by or disclosed to a relevant Northern Ireland body in connection with any devolved Northern Ireland function of the body, or*
- (b) modifies any provision made by Northern Ireland legislation where that provision deals with transferred matters.*

*(6) Any question as to which Northern Ireland department is the appropriate Northern Ireland department in relation to an information-sharing order is to be determined by the Office of the First Minister and Deputy First Minister.*

*(7) In this section “responsible Secretary of State” means the Secretary of State having primary responsibility for government policy in relation to the protection of data.*

#### *50F Interpretation of this Part*

*(1) In this Part—*

*[...]*

*“relevant policy objective” means—*

- (a) in the case of an information-sharing order made by the Scottish Ministers, a policy objective which relates to—*
  - (i) matters within the legislative competence of the Scottish Parliament, or*
  - (ii) functions conferred on the Scottish Ministers by an Act or an instrument made under an Act (whenever passed or made);*
- (b) in the case of an information-sharing order made by the Welsh Ministers, a policy objective which relates to—*
  - (i) matters within the legislative competence of the National Assembly for Wales, or*
  - (ii) functions exercisable by the Welsh Ministers, the First Minister for Wales or the Counsel General to the Welsh Assembly Government;*
- (c) in the case of an information-sharing order made by a Northern Ireland department, a policy objective which relates to—*
  - (i) transferred matters, or*
  - (ii) functions exercisable by a Minister within the meaning of the Northern Ireland Act 1988 or by a Northern Ireland department;*
- (d) in the case of an information-sharing order made by an appropriate Minister, a policy objective of that Minister;*

*[...]*

Catch-all.

***(2) In section 67 of that Act (general provision about orders etc under the Act)—***

***(a) after subsection (3) insert—***

***“(3A) In the case of orders under section 50A—***

- (a) subject to paragraph (b), subsections (1) and (2) have effect as if references to the Secretary of State were references to a designated authority (within the meaning of section 50A),***
- (b) an order made by a Northern Ireland department is to be made by statutory rule for the purposes of the Statutory Rules (Northern Ireland) Order 1979 (and subsection (1) does not apply), and***
- (c) subsection (3) does not have effect.”***

Provision in (c) merely removes a requirement for the Secretary of State to consult the Commissioner before laying regulations under the Act, which is clearly otiose, given the more elaborate theatre of the 21-day consultation.

*[...]*