Lessons on legislating for public protection information sharing: A case commentary on Christian Institute v Lord Advocate [2016] UKSC 51

GRACE, Jamie <http://orcid.org/0000-0002-8862-0014>

Published version

GRACE, Jamie (2017). Lessons on legislating for public protection information sharing: A case commentary on Christian Institute v Lord Advocate [2016] UKSC 51. Journal of Information Rights, Policy and Practice, 2 (1).

Lessons on legislating for public protection information sharing: A case commentary on *Christian Institute v Lord Advocate* [2016] UKSC 51

Mr. Jamie Grace

Sheffield Hallam University

Abstract

The decision of the UK Supreme Court in *Christian Institute v Lord Advocate* [2016] UKSC 51 temporarily undermines the Scottish initiative referred to as the 'named persons scheme' - a programme of information governance that will likely (in time) facilitate the sharing of information (and impliedly sensitive personal data) about vulnerable children in Scotland between different child welfare and public protection agencies. The Scottish government already have a blueprint, however, of the legal shortcomings of the relevant information sharing provisions of Part 4 of the Children and Young Persons (Scotland) Act 2014 (hereafter 'CYP(S)A 2014'), since the judgment of the Supreme Court in *Christian Institute* is very clear and precise in delineating exactly which information rights are lacking in specificity in the scheme as originally legislated by the Scottish Parliament at Holyrood. This case commentary piece seeks to place the decision in *Christian Institute* in a wider context with regard to the way the courts treat challenges to information sharing by public protection agencies on the basis of data protection law and/or Article 8 of the European Convention on Human Rights 1950 (hereafter 'ECHR 1950')[1].

1. Introduction and case summary

The case of *Christian Institute v Lord Advocate* [2016] UKSC 51 saw the UK Supreme Court, in a unanimous judgment, deem certain information sharing[2] provisions of the Children and Young People (Scotland) Act 2014 incompatible with the right to respect for private and family life under Article 8 of the European Convention on Human Rights 1950[3]. In essence, these provisions sought to empower the sharing of information between different child protection agencies and professionals via a 'named person' for every child in Scotland[4]. This 'named person scheme' was a core part of the 'Getting It Right For Every Child' (GIRFEC) programme rolled out by the Scottish government[5], with information sharing at the heart of the multi-agency approach this particular strategy required and indeed, championed[6]. Not due to come into force until 31st August 2016, some parts of Scotland had already seen the policy rolled out before the setback for the Scottish government in the Supreme Court[7]. In response to this judgment an order halting the coming into force of the relevant provisions of the 2014 Act has been laid before the Scottish Parliament.

---

[1] The European Convention for the Protection of Human Rights and Fundamental Freedoms 1950

[2] In this case commentary, 'information sharing' should be taken to mean the sharing between two or more public bodies or their private-sector partners, of personal data, whether sensitive or not, as defined by the Data Protection Act 1998, where those (hybrid) public bodies are data controllers and/or data processors; and for the purposes of S.6 of the Human Rights Act 1998; and for the purposes of EU data protection law, as well as other relevant EU law, including the Charter of Fundamental Rights of the European Union.

[3] The qualified right to respect for private and family life, in this case.

[4] See http://www.gov.scot/Topics/People/Young-People/gettingitright/about-named-person (accessed at 26.08.2016)

[5] See http://www.bbc.co.uk/news/uk-scotland-scotland-politics-35752756 (accessed at 26.08.2016)

[6] See http://www.gov.scot/Topics/People/Young-People/gettingitright/named-person/top-ten (accessed at 26.08.2016)

[7] n 3

The Christian Institute argued that a system of universal social care support in the form of 'named persons', based upon multi-agency work (through a single professional point of contact and public protection information sharing where necessary) was too intrusive into parents' autonomy and parental decision-making[8] - a claim (still) consistently resisted by the Scottish government[9]. The Christian Institute had suffered two legal defeats (in the Court of Session, in both Outer[10] and Inner[11] Houses), as well as seeing a bid (from Scottish Conservatives MSPs) to stop the scheme then rejected by Holyrood itself[12], before making their successful appeal in the Supreme Court. The Scottish government, however, are determined to press ahead with the policy and will no doubt be introducing revised legislation accordingly[13]. This case commentary focuses on the human rights arguments that delivered that success for the Christian Institute, since the ramifications and lessons learned from these are more applicable across the whole of the United Kingdom. But first we should turn to the particular argument advanced in the case by the Christian Institute that concerned devolved legislative competence.

The first ground of the claim was that the information sharing provisions in Part 4 of the CYP(S)A 2014 were outside the legislative competence of the Scottish Parliament, which had created it, since (it was argued) they intruded unlawfully on a reserved matter, namely the statutory framework dealing with an aspect of European Union law in the form of Directive 95/46/EC as well as the Data Protection Act 1998, specifically. The Supreme Court also rejected this aspect of the claim, since they held that the provision of the 2014 Act did not amend the 1998 Act, but rather interplayed and interconnected with it (albeit in a complex manner indeed[14]). The aim of the information sharing provisions of the CYP(S)A 2014, the Supreme Court held, was to facilitate the child protection and social care aims and objectives of the Act as a whole. In this way, the Scottish Parliament had not strayed into legislating on a reserved matter in the form of the adoption and deployment of EU data protection law. The Supreme Court explained that (across paras. 64-66):

> "[64]…It is true that the ultimate aim of Part 4 is to promote the wellbeing of children and young people. Its more specific objective is to alter the institutional arrangements, and the legal structure of powers and duties, governing cooperation between the different agencies which deal with children and young people, so that they work collaboratively, with the named person playing a coordinating role. That objective reflects the concern, noted in the background material to the 2014 Act, that a weakness in the existing arrangements was that information was not shared until the stage had been reached where a child or young person was at risk of harm. Part 4 is designed to address that concern by ensuring that information is shared between the relevant agencies, and acted on where appropriate, before that stage is reached. Accordingly, although Part 4 contains provisions whose objective is to ensure that information relating to children and young people is shared, that objective is not truly distinct from the overall purpose of promoting their wellbeing, but can be regarded as

[8] See http://www.christian.org.uk/news/victory-supreme-court-rules-named-person-scheme-illegal/ (accessed at 26.08.2016)
[9] See http://news.scotland.gov.uk/News/Named-person-orders-laid-before-Parliament-295a.aspx (accessed at 26.08.2016)
[10] [2015] CSOH 7
[11] [2015] CSIH 64
[12] See http://www.digitalhealth.net/shared_care_records/48000/recovery-plan-for-child-protection-information-sharing (accessed at 26.08.2016)
[13] See http://news.scotland.gov.uk/News/Supreme-Court-rules-on-named-person-279f.aspx
[14] [63-66]

> consequential upon it… [65] To the extent that Part 4 of the 2014 Act affects the way in which the data protection regime under the [Data Protection Act] applies to matters falling within its scope, that possibility is contemplated by the DPA itself, in section 35 ['Disclosures required by law or made in connection with legal proceedings']… [66] For these reasons, we are not persuaded that the provisions of Part 4 relate to the subject-matter of the DPA and the [Data Protection] Directive."

The substantive, human rights-oriented ground argued by the Institute *was* successful, however. This commentary turns to consider this key element of the judgment in *Christian Institute* after a more general overview of the context of information sharing by public protection agencies (or 'public protection information sharing'[15]) in the next section.

2. The context of public protection information sharing

The Law Commission has observed that in the context of the sharing of information (that is, personal data) between public bodies, often in public protection or child welfare contexts, practice must conform to the standards of up to seven discrete areas of the law - and that was a conclusion they reached before it was widely acknowledged that the Charter of Fundamental Rights of the European Union 2000[16] was justiciable in the UK courts in relation to matters of EU law, and claimants began to use the provisions of the Charter to have elements of UK statute disapplied[17], on the basis of the proper protection of their privacy rights under the Charter[18]. The Law Commission expressed this multi-partite requirement for lawful information sharing as follows:

> "In making a decision on the disclosure of information, a public body must consider the following areas of law and regulation:
>
> (1) Does the disclosing public body have the power to disclose the information?
> (2) Does the recipient public body have the power to receive the information?
> (3) Additional statutory controls on information disclosure.
> (4) The common law of confidentiality.
> (5) The Human Rights Act 1998 and the right to respect for privacy and family life under Article 8 of the European Convention of [*sic*] Human Rights.
> (6) The operation of the Data Protection Act 1998 and the underlying 1995 Data Protection Directive, including the codes, guidance and enforcement policy of the Information Commissioner's Office.
> (7) Additional professional or sector-specific duties and obligations arising from rules or codes adopted by professional, disciplinary or regulatory

[15] For a discussion of the concepts of public protection information sharing, see Jamie Grace, 'Privacy, stigma and public protection: A socio-legal analysis of criminality information practices in the UK', *International Journal of Law, Crime and Justice* (2013) 41(4), 303-321.

[16] Charter of Fundamental Rights of the European Union, Official Journal of the European Communities (2000/C 364/01), December 18, 2000

[17] For an early example of the CFREU being used in the UK to provide a substantive ground of review in the context of a data protection challenge, see *Vidal-Hall v Google Inc.* [2015] EWCA Civ 311.

[18] *Ibid*, art. 7 and art. 8.

bodies."[19]

This is a complex checklist for public bodies to bear in mind, was described in the Law Commission report as 'fragmented and complex'[20]. Statutory avenues of personal data sharing then become an advantage, as they will often preclude challenges to the information sharing under traditional *ultra vires* grounds, or the common law of confidentiality. It should be noted however that even when a statutory framework for complex information sharing across part of the public sector is created, Codes of Practice will often be required to take into account the subtleties required of information sharing (such as the facilitation of opportunities for objections to information sharing, where practicable) in the light of the more thematic, principled elements of the information law landscape i.e. Article 8 ECHR 1950[21].

Public protection information sharing can however be very much an informal activity in certain contexts, and can take place without regard to any Code of Practice, of course, since the investigation of crime depends upon the supply of information about suspects to the police, and is catered for the by exception to most data protection principles contained in s.29 of the Data Protection Act 1998. This was demonstrated in the recent case of *Bangura v Loughborough University* [2016] EWHC 1503 (QB), where a response to a police request by telephone for the personal data of a suspect was used to trace a student accused (and later exonerated) of rape, with Loughborough University sharing the address information on the student's registration form. The University had a privacy policy in place stating that only written requests for information from the police would be dealt with or would result in the sharing of personal data of students, and the police had made only a request by telephone only, but due to the effect of S.29 of the 1998 Act the disclosure was deemed lawful by the High Court, and neither in breach of the DPA 1998 nor in breach of contract.

'Oppressive', discriminatory or politically-motivated access to personal data by state agencies in the name of public protection or child welfare concerns will result in judgments in favour of the privacy of the data subjects, as is suggested by the outcome of the human rights case of *Avilkina v Russia* (2013) 35 B.H.R.C. 208 (para. 47). In this case the European Court of Human Rights readily found a violation of Article 8 ECHR 1950 where the Russian prosecutor concerned had, without seeking patient consent, accessed the medical information of Jehovah's Witnesses who had refused blood transfusion treatments.

Unlawful data sharing concerning citizens need not be oppressive to be unlawful: even good governance, if underpinned by less-than-precise information sharing provisions in legislation, will produce potential findings of unlawfulness in the same manner as *Christian Institute*. This could be because of unforeseen disproportionate or 'blanket' information sharing, or a lack of notification for data subjects, etc. depending on the exact circumstances.

On the notification principle, and turning to a matter of general EU data protection law, rather than European human rights law, in the case of *Bara and others v Preşedintele Casei Naţionale de Asigurări de Sănătate and others* [2016] 1 C.M.L.R. 41 the Court of Justice of the European Union (CJEU) determined that unclear legislation which facilitates the sharing

[19] Law Commission, *Data Sharing Between Public Bodies: A Scoping Report*, Law Commission: London. 2014, Law Com No 351, p.50.
[20] *Ibid*, p.49.

[21] See Jamie Grace & Mark Taylor, 'Disclosure of confidential patient information and the duty to consult: The role of the Health and Social Care Information Centre', *Medical Law Review* (2013) 21(3), 415-447.

of sensitive personal data from health institutions to other government bodies, and vice versa, does not fulfil the standard criterion that data subjects must be informed about the flows of information about them between such bodies, under Article 10 of the European Data Protection Directive[22]. The CJEU noted that the principle of notification was vital - since knowing about the movement of data concerning oneself is what allows for an application for its rectification or deletion to be made.

Even when a public protection information sharing initiative, or a single instance of such information sharing, does not sustain a strong legal challenge, the 'court of public opinion' can sometimes frustrate such plans. For example, from 2007 onwards, the child protection database known as ContactPoint struggled to win around public opinion, whilst government failed to allay fears over issues with the broad range of access to the data of children that it would have facilitated for caring professionals with public protection roles, which eventually resulted in the programme being halted[23]. Likewise, the NHS care.data programme of planned health data linkage across the UK struggled in the face of determined pro-privacy campaigning opposition focused on issues of individual consent for and notification in relation to patient data sharing[24], and has recently been halted in the same fashion[25]. There is to be a consultation over patient consent models that will underpin a/another new approach to health informatics now running at the time of writing in August 2016[26].

---

[22] Article 10 of the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on 'the protection of individuals with regard to the processing of personal data and on the free movement of such data' demands that "Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:

"(a) the identity of the controller and of his representative, if any;

"(b) the purposes of the processing for which the data are intended;

"(c) any further information such as

"- the recipients or categories of recipients of the data,

"- whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,

"- the existence of the right of access to and the right to rectify the data concerning him in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject."

[23] See http://www.digitalhealth.net/shared_care_records/48000/recovery-plan-for-child-protection-information-sharing (accessed at 26.08.2016)

[24] See Mark Taylor, "Information governance as a force for good? Lessons to be learnt from care. data." *Script Ed* 11.1 (2014): 1-8.

[25] See https://www.theguardian.com/technology/2016/jul/06/nhs-to-scrap-single-database-of-patients-medical-details (accessed at 26.08.2016)

[26] See https://www.gov.uk/government/consultations/new-data-security-standards-for-health-and-social-care (accessed at 26.08.2016)

In England, the post-ContactPoint approach to information sharing in child protection contexts, the Child Protection Information Sharing scheme[27], has been struggling with implementation as an IT system[28], but is at least legally underpinned by information sharing powers stemming from the Health and Social Care Act 2012, in particular aimed at facilitating public protection work involving health data of children[29].

While the court of public opinion proves dangerous to public protection information sharing programmes, particularly of the IT-system variety, and when privacy advocates and experts rightly highlight risks of potential privacy breaches, then the judgment of the Supreme Court in *Christian Institute* also shows that there are particular legal issues around compliance with Article 8 ECHR 1950 that can and will upset government programmes in this area. As a result, the core of this case commentary, and the next section, below, focuses on the tests applied from Article 8 to the information sharing provisions of Part 4 of the Children and Young Persons (Scotland) Act 2014 in *Christian Institute*.

3. The discussion of Article 8 ECHR in *Christian Institute*

Article 8 of the European Convention on Human Rights protects the qualified right to respect for private and family life. The Supreme Court in *Christian Institute* was satisfied that the provisions of the CYP(S)A 2014 placed under their scrutiny would engage this right if drawn upon by the sharing of information through or via a 'named person' for a child, and when as a result information was shared across the networks of public protection and child welfare agencies in any given part of Scotland. In finding that the information sharing provisions of Part 4 of the CYP(S)A 2014 engaged Article 8 ECHR in a manner that was unlawful, the Supreme Court observed that the complexity of the interaction between the rules contained within the 2014 Act and the Data Protection Act 1998 was unfathomable to enough of a degree so as to render the provisions of Part 4 not 'in accordance with the law' for the purposes of Article 8 ECHR. As the Supreme Court noted [para. 79]:

> "In order to be "in accordance with the law" under article 8(2), the measure must not only have some basis in domestic law - which it has in the provisions of the Act of the Scottish Parliament - but also be accessible to the person concerned and foreseeable as to its effects. These qualitative requirements of accessibility and foreseeability have two elements. First, a rule must be formulated with sufficient precision to enable any individual - if need be with appropriate advice - to regulate his or her conduct…"

The concern of the Supreme Court as to a lack of accessibility and foreseeability of the operation of the information sharing provisions under part 4 of the 2014 Act came about because of the [para. 83] "logical puzzle arising from sections 23(7) and 26(11) [of the 2014 Act, which would still seem to bar the sharing of information when ostensibly prohibited by other legislation, such as the DPA] when read with section 35(1) of the DPA [which allows for the sharing of public protection information, for instance, when required by another piece of legislation, such as the 2014 Act, albeit with the provisions in place in sections 23(7) and 26(11) of that Act]". The Supreme Court further observed that [83]:

---

[27] See http://systems.digital.nhs.uk/cpis and http://systems.digital.nhs.uk/cpis/work and http://systems.digital.nhs.uk/cpis/needed/localauthfacts.pdf (accessed at 26.08.2016)
[28] n 16
[29] See Jamie Grace, "A broad discretion to share patient information for public protection purposes: statutory powers of the NHS commissioning board." *Journal of Medical Law and Ethics* 1.1 (2013): 77-83.

> "It is also necessary to ensure that the requirements of articles 7 and 8 of the Directive are met [requiring conditions as to legitimate data processing, and requiring the prohibition of the unauthorised processing of health data, amongst other things, outside of a set of exceptions], so far as information falls within its scope. There are thus very serious difficulties in accessing the relevant legal rules when one has to read together and cross refer between Part 4 of the Act and the DPA and work out the relative priority of their provisions."

Furthermore, the Supreme Court also found that there were insufficient safeguards to represent a lawful and systematic approach to ensuring only proportionate sharing of information under the provisions of Part 4 of the 2014 Act. Crucial issues were the lack of clear processes to obtain the consent of the child for information sharing where this was relevant and necessary given particular discretionary information sharing powers, and the lack of provisions placing an obligation on professionals to consult the parents of a child prior to information being shared, or to even notify parents after information about their child had been shared.

In the words of the Supreme Court, on the issue of a lack of ECHR-compliant clarity and foreseeability in the provisions concerned [para. 84]:

> "Of even greater concern is the lack of safeguards which would enable the proportionality of an interference with article 8 rights to be adequately examined. Section 26(5) requires an information holder, when considering whether information ought to be provided in the exercise of the duties in section 26(1) or (3), "so far as reasonably practicable to ascertain and have regard to the views of the child or young person". But there is no such requirement in relation to a service provider's discretionary power to share information under section 26(8). There the test is merely that the provision of the information is necessary or expedient for the purposes of the exercise of any of the named person functions. Moreover, there is no statutory requirement, qualified or otherwise, to inform the parents of a child about the sharing of information... It is thus perfectly possible that information, including confidential information concerning a child or young person's state of health (for example, as to contraception, pregnancy or sexually transmitted disease), could be disclosed under section 26 to a wide range of public authorities without either the child or young person or her parents being aware of the interference with their article 8 rights, and in circumstances in which there was no objectively compelling reason for the failure to ascertain and have regard to their views."

As to the separate question of the proportionality of the information sharing provisions in Part 4 of the 2014 Act, the Supreme Court set out the now-standard four-part test [para. 90]:

> "It is now the standard approach of this court to address the following four questions when it considers the question of proportionality:
> (i) whether the objective is sufficiently important to justify the limitation of a protected right,
> (ii) whether the measure is rationally connected to the objective,
> (iii) whether a less intrusive measure could have been used without unacceptably compromising the achievement of the objective, and
> (iv) whether, balancing the severity of the measure's effects on the rights of the persons to whom it applies against the importance of the objective, to the extent that the measure will contribute to its achievement, the former outweighs the latter (ie

whether the impact of the rights infringement is disproportionate to the likely benefit of the impugned measure)."

The Supreme Court then set out its conclusions on the presence of a 'sufficient importance', and a 'rational connection' in the spirit of the legislation concerned:

> "[91] …it can be accepted, focusing on the legislation itself rather than on individual cases dealt with under the legislation, that Part 4 of the 2014 Act pursues legitimate aims. The public interest in the flourishing of children is obvious. The aim of the Act, which is unquestionably legitimate and benign, is the promotion and safeguarding of the wellbeing of children and young persons… [92] Secondly, Part 4 of the Act is rationally connected to the legitimate aims pursued… the named person is at the heart of the Scottish Government's proposals. That person is tasked with advising on the wellbeing of a child, helping a child or parent to access a service or support, and being the single point of contact for public services in relation to the child in order to promote, support or safeguard the child's wellbeing."

The Supreme Court also found that a margin of appreciation applied as to whether there was no likely, less intrusive means that could have been laid out in the 2014 Act, since the named person scheme depends on the flow of information for its effectiveness [para. 93] :

> "The third question (whether a less intrusive measure could have been used) does not involve a court in identifying the alternative legislative measure which was least intrusive… If, as the appellants submitted in their broader challenge, a named person should be appointed in relation to a child only if the parents consented or, absent such consent, if the appointment was necessary to protect the welfare of a child who was at risk of harm, the scope for early intervention to resolve problems and for the coordination of public services in support of a child's wellbeing would be diminished."

The Supreme Court, in its last point on the proportionality issue, and having found that there was a fair balance between the potential impacts systemically of the information sharing provision of Part 4 of the 2014 Act, did however, note that [para. 101]:

> "In order to reduce the risk of disproportionate interferences, there is a need for guidance to the information holder on the assessment of proportionality when considering whether information should be provided. In particular, there is a need for guidance on (a) the circumstances in which consent should be obtained, (b) those in which such consent can be dispensed with and (c) whether, if consent is not to be obtained, the affected parties should be informed of the disclosure either before or after it has occurred. Also relevant is whether the recipient of the information is subject to sufficient safeguards to prevent abuse [of the information]."

4. The brief approach to EU law in the judgment of the Supreme Court

The Christian Institute had raised a third ground around incompatibility between the information sharing provisions in Part 4 of the 2014 Act and EU law, specifically certain Articles of the Charter of Fundamental Rights of the EU; namely "article 7 (respect for private and family life), article 8 (protection of personal data), article 14 (right to education) - particularly 14(3): respect for the right of parents to ensure that the education of their children conforms with their convictions - and article 33(1) (family and professional life) [102]".

However, the Supreme Court felt it did not need to address this particular ground of the claim by the Institute, on the basis that:

> "In so far as the challenge relates to the over-riding of confidentiality of personal data (whether or not sensitive), we have addressed this in our discussion of article 8 of the ECHR. In *Volker und Marcus Schecke GbR and Hartmut Eifert v Land Hessen* (Cases C-92/09 and C-93/09) [2010] ECR I-11063, the Court of Justice of the European Union (Grand Chamber) held (para 52) that the limitations which may lawfully be placed on the right to the protection of personal data correspond to those tolerated in relation to article 8 of the ECHR. We are therefore satisfied that there is no additional incompatibility with EU law beyond that which we have found in relation to article 8 of the ECHR."

In addition, the Christian Institute had also argued that there was (in an unlawful manner) no obvious process under the relevant provisions in Part 4 of the 2014 Act that explained how data might be removed from the control of a named person, or prevented from being processed by them - that is, through deletion etc. However, the Supreme Court determined that the regular process of applying for an enforcement notice through the Information Commissioner's Office, or even applying for a remedy through judicial review, would suffice [para. 105]:

> "Part V of the DPA empowers the Information Commissioner, whether at the request of a data subject or otherwise, to enquire into a data controller's compliance with the data protection principles. Under section 40 of the DPA, the Information Commissioner is empowered to serve an enforcement notice on a data controller to require such compliance. The DPA thus has protections for a data subject, who can also, if necessary, seek judicial review of a decision of the Information Commissioner. In our view, the data subject is thereby given a legal remedy and judicial protection as required by *Schrems v Data Protection Comr* (Case C-362/14) [2016] QB 527, para 95."

5. The reaction to the outcome of the Supreme Court judgment

Following the judgment in *Christian Institute* there were calls for the complete abandonment of the named person scheme from pressure groups and campaigners[30], and other calls for older children to be removed from the ambit of the scheme[31]. The Nursing and Midwifery Council, with its UK-wide role, for example, pointed out that professional Codes of Practice, such as their own, create tension with government programmes such as the 'named persons scheme', since such professional Codes require individuals to carefully consider standards of confidentiality and privacy protection even as information sharing channels may open up in the future in public protection contexts; the named persons scheme in Scotland amongst them[32].

In late August 2016, nearly a month after the judgment, Deputy First Minister for Scotland, John Swinney, commented that:

> "In its judgment [of July 2016], the Supreme Court dismissed a number of challenges to the named person policy and described its aims as 'unquestionably legitimate and

[30] See http://www.bbc.co.uk/news/uk-scotland-scotland-politics-36933204 (accessed at 26.08.2016)
[31] See http://www.bbc.co.uk/news/uk-scotland-scotland-politics-36985399 (accessed at 26.08.2016)
[32] See https://www.nmc.org.uk/news/news-and-updates/statement-on-scotland-legal-ruling/ (accessed at 26.08.2016)

> benign'. However, the court's ruling made clear the Scottish Government needs to amend the information-sharing provisions in the 2014 Act and provide greater clarity about the basis on which information will be shared to ensure compliance with the ECHR… We remain firmly committed to implementing the named person service to support children and their families. We will engage with key partners across public services, the third sector, Parliament and the wider public to take this forward."[33]

Continuing to take forward the named persons component of the 'Getting It Right For Every Child' programme in Scotland thus begs a question: What lessons can Holyrood and other legislators learn from the *Christian Institute* judgment, when it comes to putting together a checklist of items and issues for inclusion and consideration in drafting information sharing provisions for legislation aimed at service delivery or transformation in the public sector, particularly in the context of 'public protection networks'[34]?

6. Lessons on legislating in order to facilitate public protection information sharing

For the devolved legislature in Scotland it is a positive that following *Christian Institute* any information sharing provisions they create will likely not now be deemed outside their legislative competence, given the outcome of the case on the issue of whether such provisions affect or impliedly amend the Data Protection Act 1998. But there is a broader set of key points to learn from with regard to the judgment of the Supreme Court in *Christian Institute*.

Clear statutory avenues of public protection information sharing can be laid down in the law by Parliament. Where avenues of public protection information sharing are *not* clearly laid down in statute, however, then the courts can be expected to protect privacy or indeed, parental autonomy, where the intrusion by one state agency or body into the private life of a family is particularly stark. Clarity in information sharing provisions, *Christian Institute* spells out for us, is necessarily, under Article 8 ECHR, a matter of recognising appropriate, qualified rights to be consulted, and/or to be notified, of information sharing - as well as recognising and ensuring safeguards aimed at keeping information sharing secure and proportionate - and laying these protections and entitlements down in the law itself, even *ad nauseam*, if that is what the law requires.

[33] See http://news.scotland.gov.uk/News/Named-person-orders-laid-before-Parliament-295a.aspx (accessed at 26.08.2016)

[34] See Sir Ian Magee, *Review of Criminality Information: Executive Summary and Recommendations*. Review of Criminality Information, 2008, and Jamie Grace, "Privacy, stigma and public protection: A socio-legal analysis of criminality information practices in the UK." *International Journal of Law, Crime and Justice* 41.4 (2013): 303-321.