Developing a Public Interest Mandate for the Governance and Use of Administrative Data in the United Kingdom

JOURNAL OF LAW AND SOCIETY
VOLUME 43, NUMBER 3, SEPTEMBER 2016
ISSN: 0263-323X, pp. 360–92

Developing a Public Interest Mandate for the Governance and Use of Administrative Data in the United Kingdom

GRAEME LAURIE* AND LESLIE STEVENS*

This article addresses the legal and ethical uncertainties surrounding the use of administrative data for research. Drawing upon best practices developed by the authors in previous data initiatives and engagement with research communities, the article suggests a problematic organizational culture as the most significant barrier to proportionate and good governance of administrative data. Accordingly, it offers a novel means for data custodians to identify key considerations by introducing a decision-making template that supports public authorities' assessment of preparedness for data reuse through identification of challenges faced, related to sector-specific practices. As a catalyst for change, the authors advocate a public interest mandate – commitment to safely and ethically use administrative data when it is in the public interest to do so. This is delivered through implementation of the decision-making template, overt commitment to principles of public interest and proportionality, and engagement with stakeholders to address remaining areas of uncertainty.

INTRODUCTION

Governments of the twenty-first century are in the business of big data. This includes the United Kingdom government, which handles 1.5 billion transactions with businesses and citizens annually.[1] Each involves *administrative* data collected for the delivery of public services, conveying a rich story

* *Mason Institute, University of Edinburgh School of Law, Old College, South Bridge, Edinburgh EH6 4DS, Scotland*
graeme.laurie@ed.ac.uk leslie.a.stevens@ed.ac.uk

This work was supported by the Economic and Social Research Council grant number ES/L007487/1 (Administrative Data Research Centre – Scotland).

1 R. Sargeant, 'Digital Marches on: Rising Take-Up, Falling Costs' (2014), at <https://gds.blog.gov.uk/2014/04/02/digital-marches-on-rising-take-up-falling-costs/>.

about British society on education, health and welfare, income, employment, migration patterns, and crime. The potential for administrative data to deepen understandings of society to better address socio-economic challenges is without question.[2]

Applying big data techniques[3] to administrative data reveals previously undiscovered patterns, relationships, and associations. It remains unknown, however, what impact such new associations have on citizens' privacy and their relationships with their governments.[4] The crucial importance of having social licence to use personal data (or even de-identified data which was once 'personal')[5] is context-specific and, as we discuss below, salutary lessons can be learned from specific sectors, such as health, where progress in governance has been achieved. Notwithstanding, within the amorphous contexts of administrative data – which implicates *all* data collected by public authorities in the United Kingdom (not just health) – the concerns are distinctive and must be recognized as such. These experiences make the United Kingdom a suitable case study for analysis of wider issues affecting many countries.

The government has made significant investment in the development of streamlined, safe, and ethical processes for drawing upon the existing resource of administrative data held across the United Kingdom's four countries. The Economic and Social Research Council (ESRC) invested £34

2 S. Koonin and M. Holland, 'The Value of Big Data for Urban Science' and R. Goerge, 'Data for the Public Good: Challenges and Barriers in the Context of Cities', both in *Privacy, Big Data, and the Public Good: Frameworks for Engagement*, eds. J. Lane et al. (2014); N. Kshetri, 'The Emerging Role of Big Data in Key Development Issues: Opportunities, Challenges, and Concerns' (2014) 1 *Big Data & Society*, at <http://bds.sagepub.com/content/1/2/2053951714564227.abstract>; Involve, 'Summary of Civil Society and Public Sector Policy Discussions on Data Use in Government' (2014), at <http://datasharing.org.uk/2014/11/07/summary-of-civil-society-and-public-sector-policy-discussions-on-data-use-in-government/>

3 Big data are often considered in terms of volume, velocity, and variety – organizations collect vast sums of data from a myriad of sources (volume); big data 'techniques' refer to the technologies underpinning big data such as sensors, database technologies, search engines, data mining, machine learning, statistics, and so on, which allow 'extremely large data sets [to] be analysed computationally to reveal patterns, trends, and associations, especially relating to human behaviour and interactions': SAS, 'What Is Big Data?', at <http://www.sas.com/en_us/insights/big-data/what-is-big-data.html>; Koonin and Holland, op. cit., n. 2, p. 137.

4 Information Commissioner's Office (ICO), 'Big Data and Data Protection' (2014), at <https://ico.org.uk/media/for-organisations/documents/1541/big-data-and-data-protection.pdf>; Law Commission, 'Data Sharing Between Public Bodies – A Scoping Report' (2014), at <http://lawcommission.justice.gov.uk/docs/lc351_data-sharing.pdf>; D. Cameron et al., 'Dialogue on Data: Exploring the Public's Views on Using Administrative Data for Research Purposes', Ipsos MORI report (2014); Goerge, op. cit., n. 2.

5 Anonymization or methods of de-identification are technical solutions and not ethical ones.

million in October 2013 to establish the United Kingdom Administrative Data Research Network (ADRN).[6] This established Administrative Data Research Centres (ADRC) in Scotland, Wales, England, and Northern Ireland, each of which would '… facilitate linkage of routinely collected administrative data, thereby stimulating opportunities for innovative research and policymaking.'[7] A key feature of the ADRN is the creation of a single governance structure to streamline robust decision making to access, use, and link administrative data for publicly funded research – a governance structure that approves projects based on their being feasible, viable, and ethical, with a clear potential public benefit.[8] To date, however, there is no gold standard for the *governance* of administrative data in the United Kingdom.[9]

Indeed, the public sector operates within a widely documented 'culture of caution' surrounding the retention and use of administrative data, where concerns are fuelled not by the law or actual procedures of data sharing but rather '… the *perceptions* of risk by all parties that will come from actually attempting to do so'.[10] The culture of caution can be understood as a culture of 'indecision' within the public sector, with the parameters for lawfully and ethically engaging in data sharing being shrouded in confusion.[11] Two studies, in particular, provide a strong body of evidence on the extent and pervasiveness of this culture of caution.[12] The first study is Thomas and Waldport's 2008 'Data Sharing Review Report' whose recommendations are based on wide consultation and extensive engagement with data custodians across public and private sectors, and with professionals and groups (including researchers, healthcare providers, academics, and so on) with direct experience of facilitating data sharing.[13] Thomas and Walport found

6 Administrative Data Research Network (ADRN), 'About Us' (2015), at <http://adrn.ac.uk/about>

7 ESRC, 'The Big Data Family Is Born – David Willetts MP Announces the ESRC Big Data Network' (2013), at <http://www.esrc.ac.uk/news-events-and-publications/news/news-items/the-big-data-family-is-born-david-willetts-mp-announces-the-esrc-big-data-network/>.

8 ADRN, 'Administrative Data Research Network – FAQs – Is the Service Provided for Commercial Use?', at <http://adrn.ac.uk/faq/about-the-process>.

9 Compare successes in the health sector such as the Scottish Health Informatics Programme. G. Laurie and N. Sethi, 'Information Governance of Use of Health-Related Data in Medical Research in Scotland: Towards a Good Governance Framework' (2012) 1, at<http://www.scot-ship.ac.uk/sites/default/files/Reports/Working_Paper_2.pdf>; Edinburgh Law School, 'Research Case Study: Good Governance for the Scottish Health Informatics Programme (SHIP)' (2015), at <http://www.law.ed.ac.uk/research/making_a_difference/ship>.

10 R. Thomas and M. Walport, 'Data Sharing Review Report' (2008) para. 6.21, at <http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/links/datasharingreview.pdf>.

11 id., p. 54.

12 id.; Law Commission, op. cit., n. 4.

13 Thomas and Walport, id., pp. 11–12.

the confusion surrounding data sharing, and in particular around legal requirements, particularly destabilizing in the public sector context.[14] However, the consultation revealed few examples where the legal framework actually *prohibited* data sharing, rather:

> The barriers, therefore, are most often cultural or institutional – an aversion to risk, a lack of funds or proper IT, poor legal advice, an unwillingness to put the required safeguards in place or to seek people's consent.[15]

The chief recommendation from this report was 'to transform the *culture* that influences how personal information is viewed and handled',[16] further emphasizing the '[failings] within institutions themselves [that] often stand in the way of appropriate information sharing'[17] as opposed to the law.

More recently, the English Law Commission undertook a similarly large-scale consultation of public authorities'[18] experience and understandings of data sharing in practice and their interpretation of the law. The objective was to identify existing impediments to data sharing which could be addressed by legal reform.[19] The Law Commission found the laws governing data sharing as overly complex and difficult to understand, perpetuating legal myths about what is prohibited or allowed and resulting in inconsistent interpretations between public authorities. A primary recommendation was therefore to begin a full law reform project to '... map, modernise, simplify and clarify the statutory provisions that permit and control data sharing and review the common law.'[20] However, like Thomas and Walport, the Law Commission recognized the impact of organizational cultures around data and the limits of law reform:

> Law reform alone will not provide the necessary solutions, but law reform can work together with and assist changes in culture and practice, for example by developing structures which facilitate good and flexible working relationships in local areas.

Within this 'data' landscape dominated by a culture of caution, even if public authorities *want* to share data for research facilitated by the ADRN, they may lack the necessary decision-making tools to distinguish between actual barriers (for example, where data sharing would be unlawful) and perceived barriers which *can* be resolved through internal changes to governance and/or dialogue with stakeholders such as staff, managers, and the public. While clarification and simplification of the law would enhance currently confused misunderstandings of what is or is not legally required to

14 id., p. 38.
15 id., p. 46.
16 id., p. 53.
17 id., p. 46.
18 As did the Thomas and Walport report, the Law Commission's report received consultation responses from private bodies engaged in public service delivery.
19 Law Commission, op. cit., n. 4, para. 1.12.
20 id., para. 1.6.

share data, this article argues strongly that additional laws cannot resolve the residual cultural and ethical issues which are unique to each public authority. These might include:

- individual and organizational reluctance to share data due to perceptions of 'ownership' of data;
- fears of public backlash over lawful but novel and ethically controversial uses of data;
- fears over reputation damage to the public authority;
- a lack of incentives, or understanding of incentives, to share data;
- a lack of clear accountability structures for data handling or senior leadership involvement; or
- a lack of formal arrangements between public authorities for sharing data.[21]

The first step towards removing unnecessary obstacles to data sharing and transforming the culture around data in public authorities is to identify real versus perceived barriers, directly confronting ethical dilemmas and pre-conceived notions as to the risks, incentives, and disincentives involved with data sharing. Public authorities in the United Kingdom are currently lacking any uniform or objective approach to distinguishing in order to undertake these tasks.

To address this unmet need, and as a crucial first step towards the development of a good governance framework for administrative data, this article introduces a tool – a decision-making template – that consolidates the complex legal and ethical considerations at stake when data custodians must decide whether to permit use of administrative data for research purposes. The template provides a concise and generalizable illustration of the key legal, ethical, and cultural scenarios data custodians may face when considering granting access to administrative data for research, or indeed for any other purpose not contemplated at the time of data collection. The template facilitates an assessment of preparedness for data sharing vis-à-vis the identification of real (versus perceived) barriers operating within their organization. In this respect, it is a form of maturity model. Importantly, the template allows data custodians to distinguish between different types of considerations, helping to reveal when – or whether – law is the 'problem'. As explained below, existing research and our engagement with stakeholders to date reveal that most often data custodians are impeded by cultural-organizational barriers that prevent proportionate data use.[22] By exposing

21 An amalgamation of 'cultural' barriers taken from the Law Commission and Thomas and Walport report. Thomas and Walport, op. cit., n. 10, pp. 41–42, 46–48; Law Commission, op. cit., n. 4, paras. 7.1–7.9.

22 Thomas and Walport, id., pp. 46–8; The Law Commission, id.; M. Oswald, 'Share and Share Alike? An Examination of Trust, Anonymisation and Data Sharing With Particular Reference to an Exploratory Research Project Investigating Attitudes to Sharing Personal Data With the Public Sector' (2014) 11 *SCRIPTed*, at <http://script-ed.org/wp-content/uploads/2014/12/oswald.pdf>; R. Wilson and A. Gray,

this key issue, we aim to shift the focus from partial legal solutions to emphasize where real and meaningful changes can be made: to organizational culture through commitment to a public interest mandate.

The next section provides an overview of the piecemeal legal landscape governing administrative data in the United Kingdom. It reveals the irony that any 'sharing stasis' might be driven by an absence of law as much as by an inability to navigate existing law. The third section offers a deeper examination of likely concerns, leading to the development of the decision-making template that sits at the heart of this contribution. The fourth and final section concludes with the suggestion that the adoption of a public interest mandate through a series of key steps can help to initiate the necessary change, not only in the United Kingdom's public sector but potentially also beyond. We advocate that such a mandate ought to be reflected in an organization's mission statement, underpinned by principles of the promotion of the public interest and proportionality and supported by meaningful engagement with relevant stakeholders, including publics.

DEALING WITH ADMINISTRATIVE DATA IN A DATA-DRIVEN WORLD

Administrative data have no single, let alone overarching, legal definition. Absent this, and without agreement on which bodies perform 'functions of a public nature',[23] for this article we adopt the definition provided by the ADRN:

> Administrative data refer to the vast range of information collected by public authorities in the course of their routine operations. This includes delivery of services such as census taking, managing income tax payments, providing child protection, performing health services, running schools, monitoring crime, allocating benefits, mediating property owner and tenant disputes, administering council housing and so forth.[24]

'Information Sharing: Easy to Say Harder to Do Well' (2015), at <http://informationsharing.org.uk/wp-content/uploads/2015/06/P0248-CoE-Academic-report.pdf>.

23 The meanings of a 'public authority' or 'functions of a public nature' remain unclear where many services are now outsourced to the private sector. The implications of being considered a hybrid-public authority in performing functions of a public nature is a critical consideration given the resulting obligations under the European Convention on Human Rights, most notably, as to Article 8 and the Right to Respect for Private and Family Life. The precedent remains from *Y.L.* v. *Birmingham City Council and others* [2007] U.K.H.L. 27, in which a bright-line rule between public/private was rejected in favour of a list of considerations on a case-by-case basis. However, for the purposes of this article, the focus remains on the category of public authorities as defined under the Data Protection Act 1998, s. (1)(1) in reference to the Freedom of Information Act 2000 Schedule 1 and Freedom of Information (Scotland) Act 2002.

24 Adapted from the ADRN's definition, 'Administrative Data' (2015), at <http://adrn.ac.uk/admin-data>.

Therefore, the scope of our contribution applies to the myriad of local, regional, and national public authorities (as defined under the Data Protection Act 1998 (DPA) s. 1(1)) which collect administrative data from their regular interactions with citizens. This includes any public authority as provided by Schedule 1 of the Freedom of Information Act 2000 (FOIA 2000) or a Scottish public authority as defined by the Freedom of Information (Scotland) Act 2002 (FOISA 2002),[25] including local authorities, government departments, universities, and so on. Furthermore, reflecting our work with the ADRN, the focus is on the use of administrative data for *research* purposes where currently data are *not* being accessed from *private* sector organizations nor being made accessible *to* such organizations for their own research. In contrast, if private entities are acting on behalf of public authorities, then further distinctions must be made. For example, if private sector organizations merely process and 'hold' data *on behalf of* public authorities, they will not incur data controller obligations;[26] as such, they would be excluded from considerations here.[27] Contrariwise, if private organizations have been explicitly declared 'public authorities', for example, for the purposes of freedom of information, then the following analysis would apply. As an example, in 2015, Scotland extended their category of public authorities to include organizations funded wholly or partly by local authorities which carry out functions of a public nature – such organizations would clearly come within the remit of this article and analysis.[28]

25 Recently the FOISA 2002 definition of public authorities was extended to include organizations funded in part or wholly by local authorities in Scotland, which carry out functions of a 'public nature' including, for example, tourism-related activities, museums and art galleries, recreational facilities, and so on: Freedom of Information (Scotland) Act 2002 (Designation of Persons as Scottish Public Authorities) Order 2013 No.278, at <http://www.legislation.gov.uk/ssi/2013/278/pdfs/ssi_20130278_en.pdf>.

26 FOIA, s. 3(2); FOISA, s. 3(2); ICO, 'Outsourcing and Freedom of Information – Guidance Document – Freedom of Information Act' (2015) 17–19, at <https://ico.org.uk/media/1043530/outsourcing-and-freedom-of-information.pdf>; ICO, 'Data Controllers and Data Processors: What the Difference Is and What the Governance Implications Are: Data Protection Act' (2014) 8–9, at <https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf>.

27 The ICO gives an example where a public authority (created by statute) outsources complaints handling to another public authority. The ICO advises that the public authority with the statutory obligation to carry out the processing remains the data controller's as to data processed by the outsourced party. Importantly, '[a]n organisation cannot be both data controller and processor for the same data processing activity; it must be one or the other.' ICO, id. (2014), pp. 8–9, 14–15.

28 The Freedom of Information (Scotland) Act 2002 (Designation of Persons as Scottish Public Authorities) Order 2013 No. 278. Scotland is considering further expanding this category to include 'various organisations, including private prison contractors, providers of secure accommodation, grant-aided schools and

Mirroring the myriad types of public authorities, there are many distinct categories of administrative data. Examples include health data, which are defined by reference to a particular health status of an individual and often tied to a particular health service provider, and benefits and tax data, whereby individuals may be traced by reference to a National Insurance number and are connected to a wider set of interactions with various public authorities including Her Majesty's Revenue and Customs (HMRC) and the Department of Work and Pensions (DWP). This article applies to administrative data in its widest sense covering all potential aspects of people's lives and their interactions with public authorities.

1. *The legal landscape governing administrative data in the United Kingdom*

Normally, the potential privacy impact on citizens is the principal consideration in any decision to use personal data. To this end, the law regulates the processing of *identifiable* personal data under the Data Protection Act 1998 (DPA).[29] Personal data are:

> . . . data which relate to a living individual who can be identified —
> (a) from those data, or
> (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.[30]

The objective of the legislation is to regulate how personal data are *processed*, which in practice means any storage or use of personal data whatsoever. Moreover, if personal data are 'sensitive' according to the law then additional justifications are required, and further restrictions on processing can apply. Sensitive personal data include data relating to an individual's health, religious beliefs, political opinions, and/or racial/ethnic origin and thus can encapsulate many forms of *administrative* data. Personal data and sensitive personal data are distinguishable from *de-identified* data, which are by definition no longer identifiable to an individual, either directly or indirectly, and as such are not regulated under the DPA. The crucial consideration, therefore, is whether data remain identifiable, directly or indirectly. Importantly, this is a question of judgement and degree. In the United Kingdom, it is recognized best practice to consider data which are de-identified to the point where the risk of re-identification is only a remote possibility. However, what is considered sufficiently de-identified or anonymized remains a contentious issue within the United Kingdom and

independent special schools': Scottish Government, 'Further Extension of Coverage of the Freedom of Information (Scotland) Act 2002 to More Organisations' (2015), at <https://consult.scotland.gov.uk/freedom-of-information/foi-consultation>.

29 The Data Protection Act 1998. (Hereinafter 'DPA')

30 DPA, s. 1(1).

Europe, particularly with new perspectives being offered in the General Data Protection Regulation that will replace existing data protection legislation in 2018.[31] Moreover, and irrespective of any legal reform, re-identification is always a future possibility when existing data are shared or linked.[32] This requires that the status of data must always be kept under review.

Within this regulatory framework, and given the crucial consideration of whether data are de-identifiable, it is important to consider how administrative data fit within this scheme. This article focuses on the reuse of de-identified administrative data for research, particularly social science research under the auspices of the ADRN.[33]

The ADRN only facilitates access to administrative data available in digitized form given the security arrangements for access in secure facilities.[34] Under ADRN arrangements, data are de-identified and made available for research via a 'trusted third party' mechanism.[35] The ADRN details the robust process through which trusted third party mechanisms make de-identified data available to researchers.[36] While acknowledging wider and on-going debates regarding de-identification,[37] it is submitted that ADRN's

31 Data Protection Directive 95/46/EC, recital 26 (hereinafter 'DPD'); P. Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2009) 57 *UCLA Law Rev.* 1701; Article 29 Data Protection Working Party, 'Opinion 05/2014 on Anonymisation Techniques' (2014), at <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf>; ICO, 'Anonymisation: Managing Data Protection Risk Code of Practice' (2012) 6, at <https://ico.org.uk/media/1061/anonymisation-code.pdf>; L. Stevens, 'The Proposed Data Protection Regulation and Its Potential Impact on Social Sciences Research in the UK' (2015) 1 *European Data Protection Law Rev.* 100.

32 Ohm, id.; A. Narayanan and V. Shmatikov, 'De-Anonymizing Social Networks' (2009) *30th IEEE Symposium on Security & Privacy*, at <https://www.cs.utexas.edu/~shmat/shmat_oak09.pdf>; P. Schwartz and D. Solove, 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information' (2011) 86 *New York University Law Rev.* 1814; M. Gymrek et al., 'Identifying Personal Genomes by Surname Inference' (2013) 339 *Science* 321, at <http://www.sciencemag.org/content/339/6117/321.abstract>.

33 For ADRN, see 'Approved Projects' (2015), at <http://adrn.ac.uk/research-projects/approved-projects>.

34 The DPA applies to manual and digitized records, so long as they are part of a 'relevant filing system' and structured '… either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible' (s. 1).

35 As provided by the ADRN: 'A trusted third party is an organisation with secure facilities for matching data': ADRN, 'Trusted Third Parties', at <http://adrn.ac.uk/protecting-privacy/de-identified-data/trusted-third-parties>; Stevens, op. cit., n. 31, p. 100.

36 ADRN, id. (emphasis added).

37 Ohm, op. cit., n. 31; Narayanan and Shmatikov, op. cit., Schwartz and Solove, op. cit., Gymrek et al., op. cit., all at n. 32; Wellcome Trust, 'Research Funders Outline Steps to Prevent Re-Identification of Anonymised Study Participants' (2014), at

arrangements would meet standard best practice whereby effective de-identification need not be risk free (which is arguably unattainable) but instead ensure that re-identification is beyond a remote possibility.[38]

The on-going challenge for data controllers, however, is whether they are willing and ready to subject their data to such processes. ADRN provides a means to navigate data protection law safely and responsibly, but the infrastructure requires the confidence and the data of public authorities in order to do so.

(a) Beyond data protection: flexibilities and inflexibilities in the law governing administrative data

Beyond data protection, public authorities must also consider a broad range of laws governing their activities.[39] Such administrative laws prescribe the purposes to which administrative data can be put either expressly by statute (laws often termed as 'gateways'), impliedly, or under common law. A public authority created by statute, such as the HMRC, does not have authority outside what is provided in its governing legislation – it must have implied or explicit statutory authority to act and therefore to use or share data.[40] This is in contrast to government departments, such as DWP, which has authority from both applicable legislation *and* from common law. The DWP, in fact, has over 63 legislative 'gateways' to share data with others. Importantly, for both statutorily created public authorities and government departments,[41] these administrative laws apply *regardless* of whether or not data are 'identifiable' under the DPA.[42] Thus, when considering whether administrative data can be shared, it is common practice first to consider the class or kind of entity that holds the data because this determines the legal basis upon which the public authority may act. In this way, the standard set of considerations is inverted within the public sector: here it is public

<http://www.wellcome.ac.uk/News/Media-office/Press-releases/2014/WTP055974.htm>; S. Barocas and H. Nissenbaum, 'Big Data's End Run Around Anonymity and Consent' in *Privacy, Big Data, and the Public Good: Frameworks for Engagement*, eds. J. Lane et al. (2014).

38 ICO, op. cit., n. 31, p. 6; Stevens, op. cit., n. 31, p. 100.

39 The notion of 'public authorities' vis-à-vis quasi-public bodies (that carry out 'functions of a public nature') is subject to the precedent in *Y.L.* v. *Birmingham City Council and others*, op. cit., n. 23.

40 The Law Commission provides a case study analysing the difference between statutorily-created public authorities such as HMRC and government departments such as the DWP using common law powers: Law Commission, op. cit., n. 4, pp. 118–46, 148–62.

41 Other public authorities with powers under common law include Ministers of the Crown and Parliament, and in Scotland, Scottish Ministers via the Scotland Act 1998, s. 53.

42 Ministry of Justice, 'The Data Sharing Protocol: Annex H, Legal Guidance on Data Sharing' (2012), at <http://www.justice.gov.uk/downloads/information-access-rights/data-sharing/annex-h-data-sharing.pdf>.

permission first, privacy second. This has important cultural-organizational consequences.

Statutory powers, whether explicit or implicit, should be considered in contrast to common law powers, which are reserved for Ministers of the Crown, the Westminster parliament and government departments in the United Kingdom. Often seen as the 'third source' of power, common law is understood '[a]t its widest … as the Crown having all the capacities and powers of a natural person, subject to the ordinary law and limited to the extent that there is express statutory provision.'[43] However, in practice, this concept, in part promulgated by the 'Ram Doctrine',[44] is limited by uncertainty as to the extent of common law powers and the lack of precedent (and thus confidence) to rely upon them to justify data sharing. In contrast, common law powers may be more flexible because they obviate the need to point to express statutory powers to legitimate use of data. In some hybrid cases, such as the DWP, legal complexity arises because of the confusing mix of statutory and common law powers, with the added dimension of whether there are explicit, implicit or silent measures addressing administrative data use. Importantly, the Law Commission concluded from its consultation with various public authorities that the absence of express (and obligatory) authority makes it unlikely administrative data will be used.[45]

It follows from the above that interpretation of statutory and common-law powers has a crucial impact upon whether authority to use administrative data is understood – or perceived – to be present. Yet more complexity is added when considering the role of guidance provided to public authorities on data sharing. This might not hold the force of law but nevertheless has crucial influence over data practices. Consider the government's guidance on the use and sharing of social security data between the DWP and local authorities: this provides that local authorities '… must not act outside their statutory powers' and '[a]ccount must be taken of any specific data sharing legislation that applies to the function being undertaken'.[46] This guidance generates uncertainty as to what extent administrative data linkage *can* be permitted under an *implied* statutory power as opposed to an *explicit* statutory power.

Crucially, it is a general principle of law that silence is permissive: that which is not prohibited is not unlawful. Practically, however, silence and non-explicit frameworks (or co-existing frameworks) create uncertainty and, often, stasis. This is compounded by the juxtaposition of examples where express legal power to share *is* given. It is understandable, therefore, that this

43 Law Commission, op. cit., n. 4, p. 85.
44 400 *H.C. Debs*., col. WA12 (25 February 2003).
45 Law Commission, op. cit., n. 4, p. 76.
46 DWP, 'Data Sharing Guidance for Local Authorities on the Use of Social Security Data' (2010), at <https://www.gov.uk/government/publications/data-sharing-guidance-for-local-authorities>.

might lead to an inference of illegality or impermissibility in *all* other contexts. But it is important to understand that this is a matter of perception and cultural resistance, not necessarily an issue of law. Nevertheless, uncertainty surrounding the law in this area is inescapable and it perpetuates cautious decision making and inhibits organizational cultural practices, as pointed out by numerous notable sources.[47] Furthermore, evidence also suggests that even *with* the weight of express statutory powers, mere legal permission to reuse data is not enough to outweigh data custodians' hesitancy to undertake any perceived risks or other costs associated with administrative data use or sharing.[48] This highlights a key distinction between law operating to mandate sharing, and law leaving open an opportunity to facilitate sharing.

Nevertheless, a general and permissive legal gateway to share data by the government has been mooted in three discrete areas (including for research and statistics),[49] but this remains at the development stage.[50] The problem in the meantime is two-fold: (i) how should data custodians proceed in navigating the current landscape? and (ii) more broadly, should we continue to imagine that a legal solution could deliver a *complete* solution to the challenges that decision-makers face? In the next section, we briefly answer 'no' to the second of these questions, before proceeding to offer a more detailed answer to the first.

FACTORS INFLUENCING ADMINISTRATIVE DATA DECISION MAKING

We have recently argued elsewhere in the context of health data (as a sub-set of administrative data), and in the particular context of the *care.data* debacle in England, that complexities surrounding decision making to support any

47 Thomas and Walport, op. cit., n. 10; Academy of Medical Sciences, 'A New Pathway for the Regulation and Governance of Health Research' (2011), at <http://www.acmedsci.ac.uk/download.php?file=/images/project/130734957423.pdf>; Scottish Government, 'Joined up Data for Better Decisions: A Strategy for Improving Data Access and Analysis' (2012), at <http://www.scotland.gov.uk/Publications/2012/11/4166/0>; Law Commission, op. cit., n. 4

48 Law Commission, id., pp. 79–81.

49 The proposed legislation would only affect data sharing by United Kingdom government authorities and would not affect data sharing implicating devolved areas such as health, education or crime in Scotland or Northern Ireland. See Digital Government Review, 'Making Digital Government Work for Everyone' (2014) 38, at <http://digitalgovernmentreview.readandcomment.com/wp-content/uploads/2014/11/EMBARGOED_CONFIDENTIAL_MASTER-Final-Report-20141124_CLEAN.pdf>.

50 Contrast the effort of Involve, 'Data Sharing: Updates from Civil Society Engagement with the UK Government on Data Sharing' (2016), at <http://datasharing.org.uk/latest/>.

particular data initiative relate as much to addressing the social legitimacy of the enterprise as to giving it a basis in law.[51] *Care.data* was perfectly lawful under the Health and Social Care Act 2012. This made no difference to the social reaction that ensued. In other words, experience tells us that while law might be necessary it is unlikely to be sufficient to address the complexities adequately.

Rather, in determining how to proceed in the realm of data reuse, we posit that a crucial first step is to identify the *kinds* of challenges being faced. To assist data custodians in doing so, we introduce a novel decision-making template as an analytical framing device to help understand the legal, ethical, and organizational concerns at stake with such decisions (see Figure 1). Understanding the nature and full scope of concerns is integral to developing a proportionate good governance framework. Equally, it is vital to distinguish between real and perceived challenges and to assess the state of preparedness of an institution to engage in robust data reuse. More particularly, this template offers three important contributions to current discourse in information governance of administrative data:

> i) It clarifies which considerations are purely legal, a mixture of legal and ethical, and/or related to organizational culture;
> ii) It exposes those concerns which are perpetuated by legal myths or perceived controversy as opposed to those that can be adequately addressed within a proportionate governance framework for administrative data;
> iii) It expressly acknowledges an often-neglected element, namely, the problematic organizational and behavioural dynamic around data.

The template works by assisting a decision maker to reflect on and categorize underlying reasons that might underpin any decision *not* to use and/or share administrative data.

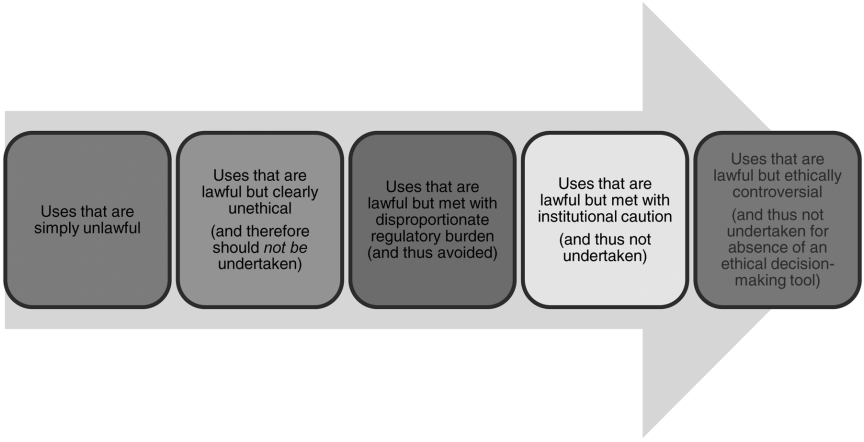
1. *Approach*

The origins of the template are found in our current research undertaken for ADRC Scotland, involving engagement with researchers and data custodians to understand existing barriers to administrative data usage. We lead the legal work package of ADRC Scotland with the aim and objective of exploring '… possible sector and country-specific solutions for delivering [interoperable information governance] involving administrative data at the local, national, European and international level.'[52]

51 P. Carter et al., 'The Social Licence for Research: Why Care.data Ran into Trouble' (2015) 41 *J. of Medical Ethics*, at <http://jme.bmj.com/content/early/2015/01/23/medethics-2014-102374.abstract>.

52 ADRN, 'Our Internal Work Packages' (2015), at <http://adrn.ac.uk/about/research-centre-scotland/work-packages> (emphasis added).

Figure 1. Administrative data decision-making template



From the outset, the nascent nature of the administrative data research field was acknowledged and we were initially guided by their previous work under the Information Governance Work Package to the Scottish Health Informatics Programme (SHIP).[53] This focused on the reuse of *health* data for research in the public interest and was taken as a legitimate example of a sub-set of administrative data. The original SHIP research and engagement with data controllers and the researcher community[54] provided an experiential and informed basis for analysing the broader culture surrounding administrative data use across public sectors in Scotland and the United Kingdom,[55] as well

53 Laurie and Sethi, op. cit., n. 9; Scottish Government, 'Joined-Up Data For Better Decisions: Guiding Principles For Data Linkage' (2012), at <http://www.scotland.gov.uk/Resource/0040/00407739.pdf>; N. Sethi and G. Laurie, 'Delivering Proportionate Governance in the Era of eHealth: Making Linkage and Privacy Work Together' (2013) 13 *Medical Law International* 168, at <http://mli.sagepub.com/content/13/2-3/168.abstract>.

54 M. Aitken et al., 'Public responses to the Scottish health informatics programme: preferences and concerns around the use of personal medical records in research' (2011) 65 *J. of Epidemiology and Community Health* A27; M. Aitken, 'What makes research/researchers trustworthy? Workshop Report' (2011), at <http://www.scot-ship.ac.uk/sites/default/files/Reports/What_makes_researchers_ trustworthy.pdf>; M. Aitken, 'Your Data and Health Research: SHIP Public Workshops' (2012), at <http://www.scot-ship.ac.uk/sites/default/files/Reports/Your_Data_and_Health_Research.pdf>.

55 Information Governance Working Group to Scottish Health Informatics Programme (SHIP), 'SHIP Guiding Principles and Best Practices' (2010), at <http://www.scot-ship.ac.uk/sites/default/files/Reports/Guiding_Principles_and_Best_Practices_221010.pdf>; G. Laurie and N. Sethi, 'Information Governance Of Use Of Health-Related Data In Medical Research In Scotland: Current Practices And Future Scenarios' (2011), at <http://www.scot-ship.ac.uk/sites/default/files/Reports/Working_Paper_1.pdf>; Scottish Government, op. cit., n. 53; Laurie and Sethi,

as providing theoretical[56] and practical grounding[57] in a principles-based approach to governance.

This was complemented by work outwith the health context and through novel doctrinal research situated within data protection, administrative law, and information governance literatures.[58] Important contributions include the Thomas and Walport Data Sharing Review (2008), the Administrative Data Taskforce (2012), Law Commission (2014), Ipsos Mori (2014), and the Centre of Excellence for Information Sharing (2015).[59]

To enrich this analysis, in 2014, we conducted a series of nine informal, semi-structured interviews with ADRC Scotland researchers across social science disciplines with diverse experiences in obtaining access to administrative data in Scotland and the United Kingdom. Interviewees were selected based on purposive or selective sampling, as we identified the ADRC Scotland co-investigators as an accessible constituency with relevant experience, and thus approached the interviews with this particular purpose in mind.[60] Interviewees were broadly asked: (i) what were their experiences in seeking approval for accessing administrative data in their respective research areas?; (ii) which safeguards were put in place to protect the privacy/confidentiality of data?; (iii) how data were to be accessed (remotely or in a secure setting)?; and (iv) whether they expected or experienced any particular legal or ethical obstacles in obtaining access in light of previous experiences?

Out of a pool of thirteen co-investigators we conducted nine informal interviews including researchers involved in: computer sciences research; geographical research; informatics; social health and welfare research; social

op. cit., n. 9; Sethi and Laurie, op. cit., n. 53; 'ScottisH Informatics Programme (SHIP)', at <http://masoninstitute.org/scottish-informatics-programme-ship/>.

56 R. Jackson, 'Principles versus Rules' (2004) 61 *Internal Auditor* 58; S. Arjoon, 'Striking a Balance Between Rules and Principles-Based Approaches for Effective Governance: A Risks-Based Approach' (2006) 68 *J. of Business Ethics* 53, at <http://dx.doi.org/10.1007/s10551-006-9040-6>; J. Black, 'The Rise, Fall and Fate of Principles Based Regulation' (2010) 17, at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1712862&rec=1&srcabs=1267722&alg=1&pos=1>; D. Bambauer, 'Rules, Standards, and Geeks' (2011) 5 *Brooklyn J. of Corporate Finance & Commercial Law* 49.

57 Based on original research undertaken for SHIP. Laurie and Sethi, op. cit., n. 9 and op. cit., n. 53.

58 The key literature cited in G. Laurie and L. Stevens, 'The Administrative Data Research Centre Scotland: A Scoping Report on the Legal & Ethical Issues Arising from Access & Linkage of Administrative Data' (2014), at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2487971>.

59 Thomas and Walport, op. cit., n. 10; Administrative Data Taskforce, 'The UK Administrative Data Research Network: Improving Access for Research and Policy' (2012), at <http://www.esrc.ac.uk/_images/ADT-Improving-Access-for-Research-and-Policy_tcm8-24462.pdf>; Law Commission, op. cit., n. 4; Cameron et al., op. cit., n. 4; Wilson and Gray, op. cit., n. 22.

60 ADRN, op. cit., n. 52.

work research; informal care research; and transport research. The responses can be divided into three themes: (i) those with previous (and *successful*) experience in obtaining access to administrative data; (ii) those focused on developing the technology to allow the linkage of administrative data for research; (iii) those with previous, *unsuccessful* attempts at accessing administrative data.

For one group of co-investigators, previous access had been relatively simple, so long as informed consent was obtained, therefore their concerns were more practical – for example, how would they navigate access from each local authority in Scotland (each with its own process) and how would this be different from access in the health sector? Their previous experiences were, in fact within the Scottish health sector, which has more prescribed and established frameworks for facilitating access to personal data for research. One other co-investigator had similar and straightforward experiences in the health context but would be seeking new forms of administrative data (for example, census data) but raised no particular concerns regarding access. A third co-investigator had international experience in successfully accessing administrative data and again raised no particular concerns regarding access to such data in the United Kingdom.

A group of four co-investigators were separately involved in technological-focused projects that would develop innovative data-linkage techniques for research purposes. Two out of four raised concerns as to commercial and proprietary rights to administrative data, which could raise a cost barrier to access. One raised concerns over physical access to the required data, that is, would they be able to run their required software on data from their own computers or would they have to visit the public authority in question? This same co-investigator raised issues as to legal and ethical obstacles – would data they receive already be sufficiently anonymized so as to be outwith the scope of data protection, or would they need to 'clean' the data from the public authority? If the latter, what would their liability be? A fourth and final 'technical' co-investigator raised concerns over the legal position on accessing historical administrative data, for example, where consent may or may not have been obtained at the time of collection and the future use of such data for research was not contemplated or thus communicated to individual research participants.

Two co-investigators had previous, unsuccessful experience in obtaining access to administrative data. One had experienced this at the research approvals phase, whereby the application was not approved due to concerns over the potential effect and impact on individuals whose data were to be accessed, even though data would be anonymized and re-identification or contact with individuals would be prohibited. The prospect of undergoing yet another application and approvals process was considered daunting and the research project would have to be scaled back. The second co-investigator had experienced protracted negotiations with United Kingdom government departments whereby it was unclear on what legal basis the public authorities

could share data for research purposes if there was no direct benefit or impact to the public authority.

The responses of ADRC Scotland researchers demonstrate the complexity and uncertainty surrounding access to administrative data, particularly to data outwith the health sector. Uncertainty arises in terms of the practicalities of access, the legal requirements for access, the public authority's basis for sharing, and researchers' own obligations as to data. We sought to supplement understandings of the *researcher* experience with administrative data with the experiences of a Scottish public authority being asked to grant access to data. Therefore we met with a team of staff at a Scottish public authority whose administrative data were to be requested by various ADRC Scotland researchers.[61] The public authority expressed hesitance to share data even amongst the separate divisions of its organization (which operated in distinct departmental silos) and further indicated it had little (to no) experience in granting/managing access to data to external individuals or organizations. If ADRC Scotland researchers were to apply for access to its data, the public authority was concerned as to the type of ethical approval body that would authorize use of its data and thus how a legal and ethical basis for sharing would be supported; in doing so it acknowledged the lack formal and established processes for seeking such approval so outwith the health sector.

Our engagement with researchers and public authorities in Scotland (and the United Kingdom) continues, providing current examples of the difficulties faced in obtaining access to data and related observations of cautious behaviours displayed by data custodians. Furthermore, we are privy to, and active participants in, ADRN-wide policy discussions on data access and security arrangements. We work closely with ADRN executives who lead negotiations with data custodians over access to administrative data and are regularly consulted on current issues as they arise. These observations are supplemented by our direct engagement with Scottish data custodians across the public sector. This engagement notably included a funded workshop 'Sharing Data Across Sectors for the Public Good' with data custodians, regulators, researchers, and other stakeholders. This event focused on the interoperability of governance arrangements as a means to facilitating data sharing for the public good.[62]

61 Data which are predominantly unrelated to the 'health' of individuals.

62 Using a snowball sampling technique to obtain participants, the workshop was held in Edinburgh in June 2015 and was funded by the University of Edinburgh's Knowledge Exchange and Impact Funding Scheme. The workshop was carried out with colleague Nayha Sethi from The Farr Institute @ Scotland, an organization intended to 'harness health data for patient and public benefit by setting the international standard for the safe and secure use of electronic patient records and other population-based datasets for research purposes.' The aim of the workshop was to facilitate open discussion between stakeholders on the challenges and best practices in sharing and using data across different sectors (for research that serves

Overall our analysis and conclusions, as illustrated in the decision-making template below, are informed on this theoretical and experiential basis. The engagement has driven the approach and is an example of co-production of a maturity model that reflects the challenges that were revealed. Consistent findings are that the culture of caution is real and remains a persistent barrier to proportionate governance.[63] It is from this basis that the need for a decision-making tool arose, one that could identify more clearly the root of the cautious behaviour exhibited by data custodians across the United Kingdom's public sector.

2. *Decisions, decisions, decisions*

As the decision-making template reveals, administrative data custodians are faced with at least five possible scenarios in deciding whether (or not) to use data. In the analysis that follows, we unpack what each of these five considerations means in practice for data custodians.

(a) Uses of data that are simply unlawful

We contend that contrary to the predominant focus of data custodians in the United Kingdom, represented in a vast body of literature,[64] the apparently impenetrable legal landscape is *not* the *greatest* barrier to the lawful and ethical use of administrative data.[65] In fact, the law is often quite clear on whether a proposed use of administrative data is lawful or unlawful. More-

the public good). Workshop findings will be published after a follow-up workshop in June 2016.

63 See previous discussion on the culture of caution in the 'Introduction' above.

64 The emphasis on legal barriers is particularly prevalent in public health literature, although there are clear indications of the former's impact on data sharing more generally. For example see: C. Warlow, 'Over-Regulation of Clinical Research: A Threat to Public Health' (2005) 5 *Clinical Medicine* 33; A. Iversen et al., 'Consent, Confidentiality, and the Data Protection Act' (2006) 332 *British Medical J.* 165; Thomas and Walport, op. cit., n. 10; H. Snooks et al., 'Bureaucracy Stifles Medical Research in Britain: A Tale of Three Trials' (2012) 12 *BMC Medical Research Methodology* 1; R. Al-Shahi Salman et al., 'Increasing Value and Reducing Waste in Biomedical Research Regulation and Management' (2014) 383 *Lancet* 176; Oswald, op. cit., n. 22; M. Oswald, 'Law Commission Consultation No 214 Data Sharing Between Public Bodies: Response to Consultation' (2014), at <http://www.winchester.ac.uk/academicdepartments/Law/Centre%20for%20Information%20Rights/Publications/Documents/Law%20Commission%20Consultation%20No%20214%20Data%20Sharing%20between%20Public%20Bodies%20response%20from%20Marion%20Oswald.pdf>; Law Commission, op. cit., n. 4; J. Bamford, 'Data Sharing: Dispelling the Myths to Achieve Multi-Agency Information Sharing' (2015), at <https://ico.org.uk/media/about-the-ico/events-and-webinars/1043650/data-sharing-dispelling-the-myths-jonathan-bamford-20150323.pdf>; Wilson and Gray, op. cit., n. 22.

65 It is important to contrast concerns about data use and data access. The respective literatures reveal a similar prevalence of concern about the blocking effect of law.

over, complexity should not be confused with lack of clarity. The key question here is: are there specific legal provisions that expressly *prohibit* data uses?

This requires, at a minimum, identification of the relevant legal provisions affecting the particular use in question. Absent an explicit prohibition, however, the decision to share or not to share becomes both a matter of interpretative flexibility, that is, *how* facilitatively will the legal framework be read, and a question of institutional values, that is, by references to which objectives and risks will the framework be read. If responsible data sharing is not part of these value preferences, then the implications are obvious. Moreover, establishing the basis for sharing gives way to the equally important considerations of individual privacy and data protection, which can further fuel cautious behaviour about sharing and access.[66]

These initial considerations obviously help to map out the precise legal parameters within which data custodians must operate. Considered in these terms, however, it further helps to distinguish clear legal authority versus prohibition and greyer areas, for example, revealing where the law is silent. If this last scenario prevails, data custodians are encouraged to deploy the template further to understand other explanations (and potential responses) for resistance to use.

(b) Uses of data that are lawful but clearly unethical (and therefore should not be undertaken)

A proportionate good governance framework for administrative data would require that each data use be not only lawful but also ethical. How, then, can a data custodian know when a proposed use of data is unethical? This question involves answering what it means to act ethically in the context of administrative data, for which we posit that the public interest plays a central role.

The ethical suitability of any proposed use of data rests with its ability to adhere to the core values that underpin collection of those data, which are in turn dictated by the values underpinning action within the relevant sector.[67] Administrative data are first and foremost a public resource; it is information obtained only by virtue of individuals' interaction with their government. Use of data by public authorities is underpinned by values focusing on

66 See section 'The legal landscape governing administrative data in the United Kingdom' above for discussion around the regulatory importance and implications of establishing (de)identifiability of data.

67 This references the principle of purpose limitation reflected in the DPA, Sch. 1, para. 2: 'Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.' Notwithstanding data being de-identified, it remains an ethical imperative to consider at the outset how new proposed uses of administrative data align (or conflict) with the purposes for which data were originally collected.

citizens' care and a defensible commitment to public service. These core values coincide with considerations of what is (or is not) in the public interest in context of a particular data initiative.

As mentioned above, the extent to which a proposed administrative data initiative *furthers* the public interest is determined in part by reference to the underlying values legitimizing action. We suggest, therefore, that determining whether a data initiative coincides with the public interest in this regard will offer answers to questions of ethical suitability. That is, the model of good governance we propose finds an important connection between the ethics of a data initiative and its social legitimacy, the latter contributing to a wider public interest grounding of the initiative. As we contend later, determining the public interests at stake within the context of a particular data initiative and supporting such initiatives with a clear and articulated public interest mandate, is crucial to securing the lawful *and ethical* use of administrative data that entails the important element of social licence.

This being said, specific examples where a proposed use would be clearly unethical and should not be undertaken would include uses that conflict with the public interests that underpin the operations of that particular public authority. This would entail initiatives that sacrifice the protection of individual privacy (a public interest in itself[68]) for the sake of organizational efficiencies or mere convenience related to a specific method (or amount) of data use. It would also categorize uses that only served *private* interests, rather than 'public interests' as unethical – say if data were shared with and used *only for* commercial gain by a private actor. Finally, uses that may serve public interests but require disproportionate intrusions into the privacy of individuals would also be considered unethical. This is not to suggest that there is a one-size-fits-all view of public interest; rather, it requires ethical reflection in each setting as to what counts as legitimate public interests that can support data use.

(c) Uses of data that are lawful but met with disproportionate regulatory burden (and thus avoided)

Regulatory burdens are often cited in the literature.[69] Initiatives involved in areas deemed sensitive, particularly controversial, or simply novel, will often be

68 Recognized by the Courts in England in *W.* v. *Egdell* [1990] Ch. 359; [1990] 1 All E.R. 835 and discussed further in: D. Townend, 'Overriding Data Subjects' Rights in the Public Interest' in *The Data Protection Directive and Medical Research Across Europe*, eds. D. Beyleveld et al. (2004); C. Raab, 'Privacy as a Security Value' in *Jon Bing: En Hyllest/A Tribute* (2014), at <http://bigdataandprivacy.org/wp-content/uploads/2014/08/Raab_PrivacySecurityValue.pdf>; C. Raab, 'Privacy as a Social Value and as a Security Value' in *Privacy and Security in an Age of Surveillance* (2015) 4 *Dagstuhl Perspectives Workshop 14401*, at <http://drops.dagstuhl.de/opus/volltexte/2015/4888/>.

69 For example, see Law Commission, op. cit., n. 4, pp. 49, 56, 89, 98.

faced with enhanced regulatory scrutiny or are *perceived* to require enhanced scrutiny and thus may be avoided on this basis as being disproportionate.[70] There can be various reasons for this, and once again, law is often seen to be a problem. This should be routinely questioned. For example, data protection law contains many legitimate use pathways and flexibilities. These include the argument that data use is *necessary* to the exercise of a function of the Crown, a Minister of the Crown or a government department (DPA, Schedule 2, para. 1 5(c)). Still, more directly the viability of consent could be explored (DPA, Schedule 2, para. 1; Schedule 3, para. 1 requires it to be 'explicit').

Far less common is the consideration that the proposed data initiative may weigh heavily in terms of the public interests it serves and therefore is necessary to undertake a function of the public authority in question.[71] There is, however, often a failure for such public interests to be clearly articulated to the relevant approval/authorizing bodies, or indeed *within* the bodies themselves. In other words, a clear commitment to sharing in the public interest is rarely found. The default too often is, rather, to find reasons *not* to share.[72]

Instances of reluctance to share data (for example, for research) are widely documented as being subject to delays for access, especially in the health sector.[73] The evidence of disproportionate regulatory burden is often linked to a failure to identify and take full advantage of the regulatory flexibilities already present.[74] Other examples include the disproportionate repeat of approval mechanisms, such as access and ethics committees. The

70 In context of local authorities: E. Copeland, *Small Pieces Loosely Joined: How Smarter Use of Technology and Data Can Deliver Real Reform of Local Government* (2015) 31–2, at <http://www.policyexchange.org.uk/images/publications/small%20pieces%20loosely%20joined.pdf>.

71 Referring to a basis in data protection law that legitimizes the sharing of administrative data under the DPA, Sch. 2, para. 5(d).

72 Law Commission, op. cit., n. 4, pp. 39–40; Copeland, op. cit., n. 70, p. 31.

73 T. Walley, 'Using Personal Health Information in Medical Research: Overzealous Interpretation of UK Laws Is Stifling Epidemiological Research' (2006) 332 *Brit. Medical J.* 130, at <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1336750/>; Laurie and Sethi, op. cit., n. 55; K. Pollock, 'Procedure versus Process: Ethical Paradigms and the Conduct of Qualitative Research' (2012) 13 *BMC Medical Ethics* 1; A. Rid, 'How Should We Regulate Risk in Biomedical Research?: An Ethical Analysis of Recent Policy Proposals and Initiatives' (2014) 117 *Health Policy* 409; Department of Health (DH), Jeremy Hunt MP, and National Information Board, 'National Data Guardian Appointed to Safeguard Patients' Healthcare Information' (2014), at <https://www.gov.uk/government/news/national-data-guardian-appointed-to-safeguard-patients-healthcare-information>

74 Academy of Medical Sciences, 'Personal Data for Public Good: Using Health Information in Medical Research' (2006), at <http://www.acmedsci.ac.uk/download.php?f=file&i=13206>; C. Haynes et al., 'Legal and Ethical Considerations in Processing Patient-Identifiable Data without Patient Consent: Lessons Learnt from Developing a Disease Register' (2007) 33 *J. of Medical Ethics* 302, at <http://jme.bmj.com/content/33/5/302.abstract>; Snooks et al. and Al-Shahi Salman et al., op. cit., n. 64.

resulting delays, costs, and other constraints can result in the complete abandonment of projects even if this is *counter* to clearly articulated public interests. Equivalent evidence is lacking in the administrative data context about the nature and extent of regulatory burdens experienced. However, valuable and recent contributions confirming a problem have been made by Policy Exchange on the experience of data sharing in local authorities in England; the Digital Government Review Team's 2014 report with recommendations on mobilizing data sharing as a national priority; the Law Commission's 2014 report on data sharing across public bodies; and the Administrative Data Taskforce's report in 2012 on the use of administrative data for research.[75]

Furthermore, albeit anecdotally, our own work engaging with the ADRN research community reveals that a disproportionate regulatory burden *does* affect access to administrative data. Discussions with researchers involved in ADRC Scotland revealed that access to administrative data in areas traditionally conceived as more 'sensitive', such as health research involving children, will often face significant hurdles to obtain data. This has resulted in entire projects and initiatives being abandoned. In others areas such as crime and justice, even where a researcher has received the relevant approvals from a wider governmental organization and/or university, each police force must be applied to individually whereby 'access is limited and is usually subject to detailed contractual negotiation', the onus being placed on the individual researcher to manage the approvals.[76] Further research and evidence of the knock-on effects of such regulatory burden is needed.[77]

Without a full understanding of the potential harm caused by risk-averse behaviour, data custodians will inevitably act more cautiously than may be warranted under the circumstances.[78] Moreover, without the identification and sharing of best practices of working within regulatory frameworks and of experiences of attempting to strike appropriate sectoral balance of interests, there is little prospect of improving public authorities' confidence in evolving innovative uses of data.[79] The deployment of the decision-making template offered here can help to smooth the path through approval mechanisms by supporting clearer identification of the precise issues at stake for all parties.

75 Copeland, op. cit., n. 70; Digital Government Review, op. cit., n. 49; Law Commission, op. cit., n. 4; Administrative Data Taskforce, op. cit., n. 59.

76 Administrative Data Liaison Service, 'ADLS – Administrative Data Liaison Service: Police Force Crime Records Datasets', at <http://www.adls.ac.uk/police-forces/police-force-crime-records-dataset/?detail#ds_jump_access>.

77 Identified as a priority area for engagement and research by the Labour Party as a result of their Digital Government Review Consultation and Report process, op. cit., n. 49, p. 39.

78 Law Commission, op. cit., n. 4, pp. 39–40; Copeland, op. cit., n. 70, p. 31.

79 Digital Government Review, op. cit., n. 49; Copeland, id.

(d) Uses of data that are lawful but met with institutional caution (and thus not undertaken)

Related, but distinguishable, scenarios arise where the law supports a particular data initiative but a confluence of institutional factors impact negatively. This scenario addresses factors specific to the sector or particular organizational culture that contribute to sub-optimal decision making.

The most recent and robust study undertaken to date on the culture of caution surrounding administrative data was conducted by the Law Commission in 2014.[80] The report discusses various elements of the said culture in terms of both perceived (for example, misinterpretations about legal repercussions) and actual barriers (for example, resources) to sharing administrative data. The report suggests that even where the law might impliedly permit a particular data initiative, data custodians can exhibit extreme caution for a variety of reasons that are institutionally embedded and therefore would not be amenable to change without significant cost and/or a paradigmatic cultural shift.[81] The Law Commission identified many reasons for institutional caution outwith the law:

- A lack of incentives (or understanding of already present incentives) to investing necessary resources to facilitate the use of data;[82]
- Institutional shortage of expertise, experience, and resources in the area of data management and, in particular, to dedicate towards ensuring data quality;[83]
- (Unsubstantiated) fear of individual reprisal over decisions taken as to new data initiatives.[84]

From our engagement with public authorities and work with the ADRN, we would add to this list:

- A lack of a shared organizational vision that understands the benefits of using administrative data;
- Fear over legal action against the institution if engagement in a particular initiative is 'novel' and thus legally 'untested';
- Fear over reputational damage and thus to public trust/faith in the institution if weaknesses are exposed by means of participation in a particular data initiative;[85]

80 However, Thomas and Walport's review on data sharing practices in 2008 also provide a robust body of evidence: Thomas and Walport, op. cit., n. 10; Law Commission, op. cit., n. 4.
81 Law Commission, id., p. 113.
82 id., pp. 105–6
83 id., pp. 105, 108–10, 115.
84 id., pp. 106–8.
85 The public backlash experienced post-care remains a constant concern and topic of debate with stakeholders.

- An absence of beacon examples to lead the way: why should an institution expose itself in being the first?[86]

A common theme between these various instigators of caution is the overwhelming sense of fear stemming from uncertainty – uncertainty as to incentives, as to the real risks involved, as to the consequences for 'getting it wrong', as to the public interest benefits to accrue (to either the organization itself or the relevant public). Unlike the previous scenario where regulatory burdens are likely to be (perceived to be) imposed from above, these instigators of caution are perpetuated internally by the data custodians themselves.

Institutional concerns, such as resources, risks to reputational damage, and a lack of clear incentives, can cause organizations and/or sectors to focus inwards in the name of caution when the focus could just as easily – and perhaps more appropriately – be placed *outward*, on the *public* nature of administrative data as a public resource. To move beyond a culture of caution, questions surrounding the reuse of administrative data, such as for research, could be reframed from the perspective of the public interest and the public mandate of public authorities to act accordingly. How does a particular data initiative support or detract from the public interest at stake for wider society in terms of potential and realizable benefits to particular groups, for the protection of privacy, for instilling confidence in a public authority, or for the sector's ability to deliver services to the citizenry? This, once again, requires data reuse to be seen as a core feature of the operations of a public authority – as a central priority that cannot be divorced from its obligations to deliver services as optimally as possible.

(e) Uses of data that are lawful but ethically controversial (and thus not undertaken in the absence of an ethical decision-making tool)

Finally, we come to scenarios where a data initiative may be lawful but is ethically controversial and ultimately not undertaken due to the absence of robust ethical decision-making tools. This scenario is helpfully illustrated by the suspended data initiative sector, *care.data*, mentioned above. This was a data initiative proposed by England's National Health Service (NHS), among other things, to '… extract data from NHS primary care medical records in England unless patients have purposefully opted out, in part to facilitate research'.[87]

86 See, also, Digital Government Review, op. cit., n. 49, pp. 38–41; Copeland, op. cit., n. 70, pp. 31–2.

87 NHS England, 'Frequently asked questions: care.data guide for gp practices' (2014), at <https://www.google.co.uk/search?q=To+support+patients%E2%80%99+choice%3B+to+advance+customer+services%3B+to+promote+greater+transparency%3B+to+improve+outcomes%3B+to+increase+accountability%3B+to+drive+economic+growth+by+making+England+the+default+location+for+world-class+health+services+research.%E2%80%99+&ie=utf-8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a&channel=sb&gfe_rd=cr&ei=xX8AVYOHFouK4Ab72oCYDw>; Carter et al., op. cit., n. 51.

Legislation (the Health and Social Care Act 2012) was enacted to make lawful the transfer of primary care patient records to the newly created Health and Social Care Information Centre for six specific reasons.[88] Furthermore, the NHS Constitution was amended[89] to include a pledge to:

> . . . inform English NHS patients about research studies in which they might be eligible to participate, and also, crucially, an expectation that patients would be willing to share their medical information for healthcare planning and for research purposes.[90]

In recent analysis of *care.data*,[91] one of us has contended that while the administrative and legal structure was created to carry out the *care.data* scheme, social licence was not obtained and this contributed to the resulting public controversy and postponement of the scheme. Not only are the purpose of *care.data* and its public benefit unclear, the attempts made to have dialogue a with the public were entirely insufficient (information leaflets sent out to NHS England patients were addressed to households, not individuals and often mistaken for junk mail).[92] The *care.data* initiative was (and remains) controversial and as a result was suspended: this was initially for six months and it has been further postponed for a more indefinite period.[93] We would further suggest that this initiative was flawed for a lack of the

88 'To support patients' choice; to advance customer services; to promote greater transparency; to improve outcomes; to increase accountability; to drive economic growth by making England the default location for world-class health services research': NHS England, 'Care Episode Statistics: Technical Specification of the GP Extract' (2013) 6, at <http://www.england.nhs.uk/wp-content/uploads/2013/08/cd-ces-tech-spec.pdf>.

89 NHS England, 'The NHS Constitution: The NHS Belongs to Us All' (2015) 8, at <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/170656/NHS_Constitution.pdf>.

90 Carter et al., op. cit., n. 51, p. 406.

91 id.

92 O. Solon, 'The Communication of Care.data to Patients Has Been an Absolute Shambles' (2014), at <http://www.wired.co.uk/news/archive/2014-02/07/care-data-terrible-communication>.

93 As of November 2015, the launch date of care.data has yet to be confirmed and its status uncertain. The scheme was to be trialled in four surgeries in England; however, in September 2015, this was postponed by Jeremy Hunt who asked National Data Guardian, Dame Fiona Caldicott to develop a new model for obtaining patient consent. The Department of Health appointed Caldicott as the country's first National Data Guardian in November 2014 on the back of care.data's controversial and stalled launch earlier in the year. Her role as National Data Guardian is to 'champion on security of personal medical information': DH, op. cit., n. 73; A. Matthews-King, 'GPs Prepare to Contact Patients Individually as Care.data Is Relaunched in Some Areas' *Pulse* (2015), at <http://www.pulsetoday.co.uk/your-practice/practice-topics/it/gps-prepare-to-contact-patients-individually-as-caredata-is-relaunched-in-some-areas/20010215.article#.VX768RNViko>; L. Evenstad, 'Public Trust Is Key to Sharing Health Data Successfully, Says Fiona Caldicott' (2015), at <http://www.computerweekly.com/news/4500256234/Public-trust-is-key-to-sharing-health-data-successfully-says-Fiona-Caldicott>.

necessary up-front assessment of preparedness for data reuse and a lack of ethical tools to successfully support its delivery pathway; the crucial tool being here, meaningful public and stakeholder (GPs) engagement.

The most obvious lesson is that clearing a legal path for ethically controversial data initiatives is not, in itself, sufficient. This should lead us to question whether legal solutions in the administrative data context would fare any better. Second, assistance in identifying and addressing potential ethical controversy is itself crucial for decision makers. Frameworks for ethical decision making, by definition, do not prescribe what ought to happen; rather, they facilitate reflection and justifiable courses of action, based on commonly recognized values, through meaningful and effective engagement with relevant stakeholders.[94] Often, a principles-based approach is used, by which we mean the identification, dissemination, and deployment of commonly agreed principles that embody the core values at stake and provide a uniform framework and language for deliberation on how to proceed.[95] In the context of administrative data, this turns on the elusive meaning of public interest. 'Public interest' is a term imbued with interpretative flexibility. It is neither possible nor desirable to say how it applies across a range of diverse (public) sectors. The term – and its legitimating role – must be defined and crafted by the authorities themselves in a given context. Equally, and as Taylor has argued, the citizens interacting with the sector must have good reasons to expect that public interest, and their data, will be deployed in defensible and accountable ways.[96]

The lack of and/or non-use of appropriate ethical tools can create a perfect storm of controversy even where it may be lawful and in the public interest to undertake a particular initiative. Our template suggests that, in any given administrative data-use context, if no ethical framework is in place, then one ought to be developed as a matter of urgency.

94 Public engagement played a crucial role in the development of a good governance framework for health data under SHIP and plays a similarly critical role in the research undertaken for ADRC Scotland: SHIP, op. cit., n. 55; S. Davidson et al., 'Public Acceptability of Data Sharing Between the Public, Private and Third Sectors for Research Purposes' (2013), at <http://www.scotland.gov.uk/Publications/2013/10/1304>; Laurie and Stevens, op. cit., n. 58.

95 SHIP, id.; Scottish Government, op. cit., n. 53; G. Laurie and N. Sethi, 'Towards Principles-Based Approaches to Governance of Health-Related Research Using Personal Data' (2013) 4 *European J. of Risk Regulation* 43, at <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3885861/>.

96 M. Taylor, 'Health Research, Data Protection, and the Public Interest in Notification' (2011) 19 *Medical Law Rev.* 267.

In light of the foregoing analysis, the legal, ethical, and organizational complexities involved combine to create a culture that:

- neither routinely identifies nor communicates the public interest and other benefits of using administrative data;
- does not incentivize the lawful, ethical, and safe and proportionate use of administrative data;
- does not have mechanisms to disabuse people of myths, perceived and unsubstantiated controversies, and liabilities arising from use of administrative data;
- does not invest in the resources required to support use of administrative data;
- does not provide decision makers with effective support to deliver responsible sharing as an embedded part of public sector practice

While the prospect of a general legislative gateway to share public authority data remains a possibility, the organizational culture and resulting practices that have become associated with 'data' cannot be changed with additional laws. What is required is a cultural paradigm shift within public authorities, in how data are valued and acted upon. While accepting that cultural change is a notoriously tall order, we offer some bold suggestions below that, if adopted, we believe will at least initiate the necessary paradigm shift.

1. *A public interest mandate to support the use, sharing, and linkage of administrative data*

To affect the necessary cultural shift within public authorities, something radical and experience-led is required. However, change need not be in the nature of extreme rupture; progressive institutional shifts can be initiated and driven by the adoption of a public interest mandate. Indeed, in the government's recent Digital Review, a key recommendation was to develop through consultation a set of key public interest principles to guide public authorities' decisions regarding data.[97] The public interest mandate we suggest, requires:

> (i) deployment of our decision-making template to isolate those issues that require attention (and to demystify others);
> (ii) organization-wide, overt commitment to ensuring that administrative data will be put to lawful and ethical use in order to serve the public interest (to be discussed and agreed with relevant sectors);
> (iii) meaningful engagement with relevant publics and stakeholders, reflected in actual governance practice;
> (iv) commitment to proportionality in all aspects of decision-making;

97 Digital Government Review, op. cit., n. 49, p. 39.

(v) identifying and addressing areas of remaining uncertainty and potential conflict.

Importantly, the proposed public interest mandate does *not* create an additional regulatory framework or administrative hurdle to the use of administrative data. Rather, it offers a means to assess readiness for responsible data reuse and to address the most problematic aspects of existing, disproportionate approaches to administrative data decision making by refocusing attention to those issues whose resolution are crucial to securing the public interests at stake. We address each of the mandate's components below.

(a) Adoption of the decision-making template

Deployment of the novel decision-making template is crucial to determining, in any given context, what are the real or perceived barriers to using administrative data. Public authorities must commit to dispelling false perceptions as they relate to law and to apparent individual and organizational repercussions for decisions taken in this area. Identifying and assuaging concerns will help to encourage more confident decision making in proportion to actual risks and benefits of any proposed use of data. In identifying scenarios where problematic cultural practices or attitudes to data are impeding proportionate decision making and separating those situations from actual legal barriers, *new* approaches can arise. These crucial distinctions, between real and perceived barriers, should be reflected in the training and development activities across a public authority.

(b) Organizational commitment to the principle of the public interest

In isolating the key considerations, data custodians may re-focus on the 'public interest' of any proposed administrative data initiative. As a public resource, each proposed use of data should be considered from this standpoint. Data custodians should embrace a transparent public interest mandate to effect change to how their data are valued and used – this requires publicly committing to the principle of the public interest.

The public interest must not be understood as an 'either/or' proposition between considerations of protecting individuals' privacy and broader societal interests. Rather, the public interest lies in *both* the robust protection of individual privacy and uses of data that stand to result in wider public benefit. The latter would include research uses of administrative data that can result in positive outcomes for society (for example, better public services in health, education, transportation, enhanced understanding of factors that contribute to the health and overall wellness of individuals in society, and so on).[98] An example of this kind would be for data custodians

98 Administrative Data Taskforce, op. cit., n. 59, p. 1; 'Benefits of the Data' (2015) <http://adrn.ac.uk/admin-data/benefits>.

of administrative data to commit to:

> Scientifically sound and ethically robust research based on use, linkage and reuse of administrative data is in the public interest in promoting and improving economic growth, personal and social well-being, and maximising the interests of current and future generations of citizens in the UK.[99]

A mandate might equally provide that:

> Citizens' rights of privacy will be safeguarded by robust and proportionate safeguards, in recognition of the public interests served by protecting individual privacy.

This mandate could be given substance in the mission statement of data custodians and would necessarily be different in each case, according to the remit of each public authority and their interactions with the public. Crucially, as recognized above, there is no definitive public interest; it is always to be determined on a case-by-case basis in line with the values and specific context in question. By committing to, and *being seen to* commit to the principle of the public interest, however, a shared and permeated vision can be cultivated internally and simultaneously initiate a meaningful point of engagement with the public and other stakeholders. A shared, organization-wide commitment to realizing the public benefits of the safe and ethical use of administrative data is crucial to initiating change. By *publicly* committing to serving the public interest in this way, data custodians can seek the crucial social licence by assuaging individuals' concerns about the likelihood of any data initiative being used for anything other than projects that will positively benefit individuals and society.[100] This might be further supported by clear statements and commitments about uses to which administrative data will *not* be put.

(c) Meaningful engagement with likely users and relevant publics

Law cannot prescribe social licence. It cannot be manufactured; it must be earned. This crucially involves the need to substantiate the public interests served by all uses of data.[101] Recent public attitudes research has emphasized the importance of engaging with relevant publics *early* in the process of data initiatives, as the Ipsos MORI study did for ADRN when it was established in 2013.[102] Meaningful engagement requires ongoing dialogue,

99 As originally provided in our working paper: Laurie and Stevens, op. cit., n. 58, p. 39.

100 Cameron et al., op. cit., n. 4, pp. 7, 17.

101 A key finding of the 2014 Ipsos MORI study was that participants were consistently concerned whether social research involving administrative data would actually lead to social value: id.

102 Engagement that is ongoing throughout the ADRN, such as through citizens' panels in Scotland and Wales. 'Public Engagement: Become Involved in Social Science Research' (2015), at <http://adrn.ac.uk/about/research-centre-scotland/public-engagement>.

consideration of the risks and benefits involved with processing administrative data and of how such concerns would be addressed through a principled, proportionate governance framework in which the public interest plays a vital part.

Importantly, the Ipsos MORI study found that:

> … the public would be broadly happy with administrative data-linking for research projects provided (i) those projects have social value, broadly defined (ii) data is de-identified, (iii) data is kept secure, and (iv) businesses are not able to access the data for profit.[103]

To translate these findings into *meaningful* engagement, the concerns raised must be transparently taken into account. As a good practice example, the ADRN uses a documented approvals process, which hinges upon the concerns raised by the participants in the Ipsos MORI study.[104] It is important that engagement not be tokenistic, either in practice or in perception. Engagement must have at least a reasonable prospect of having a real bearing on how data initiatives operate. All decisions, including conflicting policies and procedures, must be robustly justified.

(d) Commit to proportionate governance

Proportionality is a cornerstone principle for decision making and regulation that requires a balance of interests, relative to an assessment of real risks and likely benefits.[105] Determining whether a proposed data initiative is proportionate to the public interest aims sought is indicative of whether a data initiative is 'in the public interest'. The principle of proportionality is supported by a clear framework of assessment provided within context of the European Convention on Human Rights and decisions taken by the European Court of Human Rights.[106] Adapted to the current context, proportionality points towards the following questions:

- Is there a clear and knowable public interest served by the data initiative?
- Has the necessity of data use been demonstrated relative to the public interest?
- Has the relative intrusiveness of data use been minimized – is the least intrusive method being used?

103 Cameron et al., op. cit., n. 4, p. 57.

104 ADRN, 'Protecting Privacy: Project Approval' (2015), at <http://adrn.ac.uk/protecting-privacy/project-approval>.

105 Proportionality plays a crucial role in the good governance frameworks one of us developed in the health data context: SHIP, op. cit., n. 55; Laurie and Sethi, op. cit., n. 94; Sethi and Laurie, op. cit., n. 54.

106 *Handyside* v. *UK* [1976] 1 E.H.R.R. 737; *Sunday Times* v. *United Kingdom* (1979) 2 E.H.R.R. 245; *Sunday Times* v. *United Kingdom* (No 2) [1991] E.C.H.R. 50; *A., B. & C.* v. *Ireland* (2010) 53 E.H.R.R. 13.

- Are there safeguards against abuse and misuse of the data, including sanctions?[107]

A commitment to proportionality, including the assessment and management of real risks reduces undue regulatory burdens and helps to ensure employees across the public authority are not only trained in the risks involved and precautions to be taken, but are also made aware of the benefits of *using* data and the harm that might arise out of *not* using data.[108]

(e) Identify and address remaining areas of uncertainty

Some areas of uncertainty still remain. First, uncertainty remains as to the exact nature and scope of the risks involved. Articulating public interest benefits is only one-half of what is required in committing to a public interest mandate – any use of data must be proportionately assessed for its propensity to cause harm to individuals and other public interests. Yet, this assessment is currently extremely difficult for data custodians and this might further forestall proportionate decision making. The development of a sound evidence base across sectors must therefore also be an imperative. More research and sharing of best practices is needed. In the absence of evidence of harms, however, good-faith assessments and sound ethical reflection to promote a public interest mandate can promote the beginning of the cultural shift advocated in this article.

107 U. Kilkelly, *The Right to Respect for Private and Family Life: A Guide to the Implementation of Article 8 of the European Convention on Human Rights* (2003), at <http://www.echr.coe.int/LibraryDocs/DG2/HRHAND/DG2-EN-HRHAND-01(2003).pdf>; D. Korff, 'The Standard Approach Under Articles 8–11 ECHR and Article 2 ECHR' (2009), at < http://ec.europa.eu/justice/news/events/conference_dp_2009/presentations_speeches/KORFF_Douwe_a.pdf >.

108 The harms arising out of a failure to share data have been explored in social policy literature and in context of acute failures in social services resulting in great harm and impact to individuals and communities: see *The Victoria Climbié Inquiry* (2003), at <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/273183/5730.pdf>; 'Paedophile Jailed for Raping Girl' (2006), at <http://news.bbc.co.uk/1/hi/england/southern_counties/4926482.stm>; C. Bellamy et al., 'Information-Sharing and Confidentiality in Social Policy: Regulating Multi-Agency Working' (2008) 86 *Public Administration* 737, at <http://dx.doi.org/10.1111/j.1467-9299.2008.00723.x>; '"Mistakes Were Made." HMIC's Review into Allegations and Intelligence Material Concerning Jimmy Savile between 1964 and 2012' (2013), at <http://www.justiceinspectorates.gov.uk/hmic/media/review-into-allegations-and-intelligence-material-concerning-jimmy-savile.pdf>; A. Jay, 'Independent Inquiry into Child Sexual Exploitation in Rotherham 1997–2013' (2014), at <www.rotherham.gov.uk/.../independent_inquiry_cse_in_ rotherham.pdf>; Press Association, '"Catastrophic Failure" Allowed Convicted Killer to Murder on Day Release' (2015), at <http://www.theguardian.com/uk-news/2015/mar/23/catastrophic-failure-allowed-convicted-killer-to-on-day-release>; 'Risks Associated with Sharing/Not Sharing Information' (2015), at <http://informationsharing.co.uk/wp-content/uploads/2012/07/Risks-associated-with-sharing-information.pdf>.

Second, there is uncertainty as to the necessity of introducing new laws, as argued above. In light of Brexit, one of many unresolved questions is how the United Kingdom will proceed in updating its own data-protection regime. Whether or not it remains part of the European Economic Area (and thus bound by the forthcoming GDPR), it is likely that an essentially equivalent legislation will be adopted to withstand determinations of adequacy for data transfers between the United Kingdom and the EU. Regardless of the precise terms and conditions of Brexit, the United Kingdom is unlikely to diverge greatly from EU law in respect of data protection. As for introducing new data-sharing laws, and as the Law Commission has noted, '... misunderstanding and confusion about what the law requires can also point to a need to simplify or codify the law to address its complexity and make it more accessible to practitioners.'[109] The multitude of existing gateways for sharing and using data could be simplified into more discrete and overarching data-sharing legislation, currently being considered in an open policy process. Even so, such a legal exercise alone will not be enough to deliver the necessary culture change.

For this to be realized, the role of principled and discretionary decision making within a governance framework must be recognized. If a data custodian has to determine whether a proposed use of their administrative data is 'in the public interest', this will require exercises of judgement that are not currently supported by the problematic culture surrounding data. In this sense, sector-specific guidance that promotes public interest sharing would ideally be provided by a body with overarching authority – such as the United Kingdom's Information Commissioner's Office[110] – or other relevant, sector-specific professional bodies; this could ensure the guidance had the requisite authority and legitimacy to instil confidence. However, the challenge of cross-sector uncertainties and disparities remains. Full harmonization across sectors is highly aspirational, and probably unattainable. Rather, there needs to be mutual recognition of diverse approaches under the common objective of sharing public authorities' data in the public interest. Yet again, this requires more evidence of best practice, especially inter-sectoral best practices, and the capture and dissemination of experiences of multi-agency data initiatives that have demonstrated responsible and mutual sharing.[111]

Third, the authoritative research in this area – the Law Commission's 2014 report – only reflects the data-sharing practices and laws of England and Wales – similar scoping research must be undertaken in both Scotland and Northern Ireland, where devolved powers are likely to mean divergence in practice. This makes it even more imperative to determine the true nature

109 Law Commission, op. cit., n. 4, p. 25.

110 The United Kingdom's Information Commissioner's Office regularly publishes sector-specific guidance which often become best practice (for example, its 'Anonymisation Code of Practice'): see <https://ico.org.uk/for-organisations/>.

111 As recently considered in context of local authorities: Copeland, op. cit., n. 70.

of law's role in responsible sharing. The same is even truer if international sharing is contemplated.[112] The interoperability of governance regimes is key to success here. Initiatives such as the ADRN and Farr Institute are dedicated to this end. Further scoping work is necessary on the cross-sectoral and country-specific differences in cultural attitudes and resulting practices surrounding different types of data, data custodians, and data users in the United Kingdom and beyond.

While this article focuses on the broader components to achieving good governance across the inherently varied context of administrative data, efforts must simultaneously consider the benefits of designing frameworks built for interoperability but that are sensitive to and provide for the varying cultures, needs, and resources specific to particular public authorities arcoss the public sector.

CONCLUSION

This article has addressed the broad range of legal and ethical concerns arising out of the reuse of administrative data for research, using the United Kingdom and experience in working with the ADRN as an exemplar. It puts forward a novel decision-making template to help public authorities navigate the complexities discussed herein, and to distinguish between purely legal, ethical, and cultural factors that impact upon this process. This template crucially exposes the problems associated with legal myths and perceived controversies and how they contribute to the creation of a problematic culture of caution impacting on data use by public authorities. Our original contribution lies in linking two key elements to address cultures of caution: the deployment of the decision-making template to reveal what is at stake as a measure to assess preparedness for data reuse, and the adoption of a public interest mandate to set and deliver priorities and to promote necessary cultural shifts in attitudes and practice. As has been demonstrated, while simplifying the law in this area would certainly diminish *legal* uncertainty, the problematic culture that has arisen in context of administrative data requires separate and dedicated attention.

112 Not least because of the recent European Court of Justice decision rejecting the adequacy of the EU-United States Safe Harbor agreement: *Schrems* v. *Facebook* (2015) C. 362/14.