International access to restricted data - a principles-based standards approach

Felix Ritchie, University of the West of England, Bristol

Corresponding author: Felix Ritchie, Bristol Business School, University of the West of England, Bristol, UK. Tel: +44 (0) 11732 81319. Email: felix.ritchie@uwe.ac.uk

Abstract

Cross-border access to restricted government microdata for research has made relatively little progress. Recent developments are notable as exceptions. This paper argues that the situation is made more complex by the lack of a common general frame of reference for comparing objectives and concerns; this reinforces the risk-aversion in government organisations. Attempts to develop general international data access strategies therefore collapse to *sui generis* bilateral agreements of limited strategic value.

One way forward is to decouple implementation from strategic principles. A principles-based risk-assessment framework, using popular multiple-component data security models, allows decisions about access to focus on objectives; similarly, secure facilities could be developed to standards independent of dataset-specific negotiations. In an international context, proposals for classification systems are easier to agree than specific multilateral implementations. Moreover, a principles-based approach can be aligned with organisational goals, allowing countries to signal strategic intentions to others without the need for explicit commitment.

The paper uses examples from the UK, US and cross-European projects to show how such principles-based standards have worked on a within-country basis and may help to resolve immediate practical issues.

Keywords: Data access, data security, international agreement, standards

1. Introduction

In recent years, significant and widespread improvements have been made in the availability for research purposes of confidential microdata from government sources. Although there has been some reduction in detail in some anonymised files arising from concerns about data matching, this has been counterbalanced by an increasing range of alternative access models. Whilst implementations differ widely across countries, greater awareness of the value of such data and an increasing confidence in the ability of National Statistics Institutes (NSIs) or other bodies to manage the risks of access via an expanded toolkit of solutions means that use of confidential microdata for research is becoming the norm within developed countries.

The same cannot be said for sharing of confidential data internationally. In general, only highly aggregated data have been made available across national borders [1; 21, section VIII]. Researchers wanting to carry out multi-country studies have either had to restrict their analysis to these aggregates, or perform separate local analyses. This limits the inferences that can be drawn. For example, the ability of multinational companies to share knowledge across different markets is assumed to be a major competitive advantage; however, as no countries share microdata from businesses, analysis is based on intra-country activities. Moreover, the range of aggregates is usually restricted to those selected by the NSI, although 'live tabulation' tools (such as the one at AskCHIS: http://**ask.chis**.ucla.edu/) are addressing this.

NSIs have very limited incentives to invest resources in exploring these issues. As Ritchie et al. [14, 18] note, traditional risk/reward perspectives restrict the incentives for NSIs to release confidential data within countries. Across countries, the risks borne by and effort needed from the NSI are larger and the benefits to the NSI (such as data validation) much less direct, attenuating the risk/reward dichotomy.

This can be seen as a chicken-and-egg problem:

(a) Internationally agreed 'secure' technical solutions are not developed because the legal framework is not in place to allow this technology to be exploited

(b) Legal arguments over what is allowable are not being considered because there is no agreement on how the security of a proposal could be technically ensured

Ritchie [16] argues that law and technology are important when choosing a specific implementation, but are largely irrelevant when considering an NSI's strategic objectives. The same argument can be made here. Is it possible to develop a general framework for taking forward international data sharing, such that each NSI can make decisions consistent with objectives but implemented according to their own specific situation? In other words, can implementation be effectively 'decoupled' from objective-setting?

This paper suggests this is feasible by using a 'network' model to disentangle aims and implementation: set the functional standards, and let individuals address their own needs consistent with those standards. The framework developed in this paper is a way of describing risks and desirable outcomes, not a specification for 'the' way to do things.

In this, the paper complements [16], which argued that strategic decisions about access should be taken without direct reference to law, technology or risk; these are *enablers*, factors which can allow or constrain objectives but do not define those objectives. That paper sought to break the link between objectives and solutions; this paper reinforces that point by shifting the focus to the characteristics of solutions rather than any particular (and country-specific) implementation.

The next section describes some existing *sui generis* cross-country arrangements from Europe and North America, and the lessons that can be drawn from them. As this paper proposes using a standard-setting framework to break the legal-practical cycle, section 3

briefly reviews the literature on standards. Section 4 examines the 'decoupling' argument in more detail. Section 5proposes a specific framework and then shows how it could be used to both describe and recommend alternative security frameworks. It also looks at how such a framework copes with new technological developments such as the 'cloud' or grid computing.

This paper is about how government bodies in different countries can develop a framework for agreement. Common practice is not the objective, but may be an outcome. Section 6considers pathways to common adoption of both principles and practice on the long-term path to a true data-sharing network, and examines some of the practical difficulties that would arise. Section 7 concludes, offering some thoughts on planning horizons and whether the journey has value even if the aim is ultimately too ambitious.

The discussion is relevant to all with an interest in international data access. It is also relevant for those interested in getting agreement between risk-averse organisations within countries where regulation is infeasible; for example, many government organisations generate confidential datasets with research potential but are unwilling to share them, even with other parts of government. However, for easeof exposition this paper assumes NSIs are the data owners interested in providing access to confidential data outside their own regulatory systems.

2. Lessons from existing international data sharing

There are international situations where the first barrier described in the introduction - developing specific technical solutions without an overarching legal framework - has been overcome. Current examples include

- The IPUMS (International Public Use Microdata Series) project www.ipums.org to harmonise and share confidential but anonymised Census microdata from sixty-plus countries [12]

- 'Mesodata' models, as used in Airaksinen [2] for example, where semi-aggregated microdata are created from country-specific disclosive microdata with a view to a particular type of analysis; knowing in advance what models are to be run allows non-disclosive aggregates to be used to embody the necessary interactions

- The 'RDC-in-RDC' model, using remote access technology to allow researchers in the US to access a research data centre (RDC) at the German ministry of labour [4]; the Eurostat-supported project 'Data Without Boundaries' (DwB) is piloting the expansion of this model to the UK and France

- The Dutch statistical office's use of contractual arrangements within the umbrella of European law to allow Italian researchers to have live access to the Dutch RDC (source: conversations with Dutch NSI staff)

- The 'Lissy' remote job submission system allowing researchers around the world to run queries on confidential earnings data [11]

NSIs also make ad hoc contract arrangements with specific third parties for processing or, more rarely, analysis.

The five examples above are the results of single or repeated bi-lateral agreements. The typical model is of a small number of committed individuals convincing one or more governments to relax data access. As the legal and technical framework is usually specific to the particular case, it could appear that few general lessons can be drawn. However, it is the variety in these arrangements and the way they have been achieved that is instructive.

In no case has any specific law been passed or unique technology developed. In other words, these cases demonstrate that the feasibility of the solution has been less important than the willingness to achieve something. This is also very much the experience of within-country data access development in the past decade [16][1].

3. The role of standards and networks in co-operative development

There is a wide literature in management science on the development of standards and the roles that dynamics and the attitude of affected parties have on the outcome. Brunsson et al. [7] provide a summary and also introduce a selection of papers focusing on the organisational aspects of standard setting. Four elements of the literature, relating to tensions in the development of standards, are important for this paper.

The first area of tension is in the number of participants in the standard-setting process. More participants can increase acceptance of a standard by delivering 'input legitimacy'. On the other hand, more participants can make the likelihood of useful agreement more difficult. Examples of both cases can be found in the literature, and so the value of an 'inclusive' or 'exclusive' approach to standard development is very much case-dependent.

The second area of tension is the dynamic interaction between standard-setting and adoption or diffusion. As van den Ende et al. [9] note, the development of standards is rarely a linear process, and flexibility in development and an ability to respond to events or the interests of stakeholders may be key characteristics of a successful standard. However, a standard which is too flexible may be insufficiently specific to allow the gains of standardisation to be reached, and the standard is not widely adopted.

[1] The Eurostat-supported project 'Decentralised and Remote Access' (builds on the proposals described in Brandt [5] and does exploit changes in European regulations, but the key issue is the willingness of countries to delegate authority.

Third, the voluntary nature of the standards means that there needs to be a reason for the adoption of the standard. Ideally, this would be through the 'carrot': the standard provides positive benefits which encourages compliance. However, the history of competition between standards suggests that the 'stick' is often more effective: standards adoption is driven by those with market power who have reached the critical mass to be able to impose their interests on others. For example, one UK government department insisted that universities wishing to be recipients of sensitive administrative data for research be holders of ISO27001 certificates (the International Standards Organisation's quality marker for data security); as the department was a monopoly supplier of the information, standards-compliance was imposed.

Finally, the adoption of a standard at the organisational level does not mean that it is adopted at the operational level. The presence of an 'expert group' setting standards immediately creates a division between 'insiders' and 'outsiders', however wide the expert group; and this can lead to a lack of willingness to comply. Sandholtz [19] notes that this can be heightened when those responsible for implementing a third-party standard consider themselves equally expert in the topic and have no opportunity to contribute to decision-making processes. In the context of international standards, it is the author's experience from Eurostat meetings (where, by definition, all attendees are 'country experts') that inter-country differences allow much scope to justify non-compliance, and so significant amounts of time are spent ensuring that standards address the likely objections of non-participants.

In the economics literature, standards have received less interest, partly because the topic is seen as theoretically straightforward: if the adoption of a standard produces more benefits (which could include organisational efficiencies as well as direct financial gain) than costs, it would be adopted by the rational firm. Of more interest are the decision processes of the agent: how much effort should be expended in building a coalition of interest, whether the

network benefits of an open standard outweigh the monopoly benefits of a closed standard, how much effort should be invested in defending a standard, and so on. Again, the theory on this is relatively straightforward, and empirical analysis takes the same case-study approach as management sciences.

One area of economic analysis that is of relevance here is the role of standards as a pure information device. Many economic models typically assume a large amount of knowledge on the parts of the agents, but in models of missing information, standards have a role to play beyond the practical cost-benefit application. A standard may be the cost-effective way for an organisation to acquire the knowledge it requires for its business; it can also act as a cost-effective signal to other organisations of its own standards or activities. The interest in these cases is that it is unlikely that the organisation will have sufficient incentive to develop standards itself; there is however a benefit to society generally in developing such standards. This either encourages the formation of clubs of interested parties (if the gains to co-operating with others outweigh the gains from free-riding), or provides a case for government intervention.

In the discussion below, two 'standards' are being discussed. One is a common terminology and security model – the way of identifying the goals of data owners. The second is a set of specific 'levels of achievement' for those goals – targets which some might feel are appropriate, others might want to strengthen or relax. For clarity, we will refer to the general approach and terminology as the 'framework' (a 'process standard' in the organisational literature), and specific levels of data security as the 'standards' within that framework ('outcome standards' or 'design standards', depending on interpretation).

4. Decoupling principle from practice

There is no universal view on the appropriate technologies for sharing data internationally. This should not stop agreements on principles, but in practice negotiations usually focus on

implementation: decisions about ‘what’ and ‘why’ turn into discussions about ‘how’. The solution is to ‘decouple’ these two types of problems.

As Ritchie [15] notes, there are many different ways to provide secure access to confidential data, ranging from anonymised public-use files to remote-access research facilities and synthetic data. These have been implemented in different countries in different ways (sometimes within the same organisation; see, for example, the US Center for Disease Control’s restricted data web page at http://www.cdc.gov/rdc/). Although these are often complex solutions requiring statistical and policy judgments, the theory, techniques, and technology are all well understood. An NSI wishing to acquire a secure solution can pull one ‘off the shelf’, albeit with a need to tailor the solution to its own particular case. The key point is that an NSI can focus on its own objectives comfortable in the knowledge that a solution can be implemented, somehow.

The legal framework is usually seen as immutable, but Ritchie [16] argues that law is functionally no different from technology: it is a mechanism to ensure that objectives are implemented properly, but it should not define those objectives. The experience of the last decade in several countries demonstrates that the relationship between statute, custom, and institutional preference is rarely as black-and-white as claimed.

This is the basis for decoupling: decisions are made on principle, based upon what the NSI aims to achieve. The wide variety of ways to achieve the same end relieves the NSI from concerns about implementation, and the NSI approaches legal issues knowing what it wants to achieve. An analogy is with computer networks: a standard specifies how computers talk to each other over the internet, but the actual devices used for this are irrelevant.

For bilateral negotiations, it could be argued that this argument over whether principles or solutions are at stake is just hair-splitting, as the two parties will have to agree on a specific

solution. But the aim of this paper to is provide a basis for multilateral agreement and unilateral action; the improved efficiency may benefit bilateral discussions but does not restrict them. Again taking the example of computer networks, some organisations do have dedicated networks linking them to commercial partners. However, for most companies it is cheaper and easier to connect to the internet using open standards.

The focus on principles works because it reflects the thinking of the NSI. Although prospective collaborators may ask questions about technical security of solutions, the real underlying interest is, for example, “can my data be transferred to the internet?” Decoupling makes these questions the basis for any agreement, not any specific technology or law.

To build a general-purpose framework requires an acknowledgement that the questions NSIs ask will be different. Some will be more concerned about ensuring that the data themselves are confidentialised; others that any statistical outputs are non-disclosive; others that the system cannot be hacked into. Hence, a useful (and thus credible) framework needs to allow for multiple domains.

For the same reasons, the framework needs to have multiple levels of compliance (‘standards’) within these domains. For example, countries might disagree on what level of training is needed to make a researcher trustworthy to access very sensitive data, or on what is meant by ‘anonymised’ data. The standard does not define ‘this is what you should do’ but rather ‘*if* you do this, *this* is the security level you will have reached’. Returning to the computer analogy, a bank can use basic internet protocols for on-line banking, but if it chooses to comply with the Secure Sockets Layer protocol then it is demonstrably conforming to a known level of transaction security. This is the model of ‘tight coupling’ where compliance with a standard is a positive stage in the assurance of a project [19].

So, the task of the framework is to provide a flexible common terminology and model, and within that to identify appropriate 'output standards'. However, simply using the framework as a taxonomy (that is, to describe and classify) ultimately is of limited value. The benefit comes from using the framework as the basis for negotiation amongst groups who may have wildly differing opinions on good practice.

The key element is that details of implementation are kept to a minimum. An NSI wishing to deposit data need only consider what security questions it wants answering – the specific implementation is someone else's problem. Similarly, an RDC could identify itself as being compliant to a given standard without making a commitment to a particular technology. The framework and standards, not the implementation, become the focus for discussion and comparison.

5. The framework in practice: an example of standards and use

This section details an example framework to show how useful standards could be defined and used, and how it could be extended. This section covers:

- defining the relevant components of the framework
- defining standards that reflect objectives
- applying this to a set of extant solutions
- designing standards for new solutions
- accommodating future developments

The comments below arise from the author's experience in the UK, and from consulting with (or advising) Eurostat, the OECD, and NSIs in North America, Europe, and Oceania . It could be argued that there are too few or too many domains, for example, or that the risk assessments are wrong. These are valid points but not relevant here, where the purpose is to illustrate the way forward using a familiar model.

5.1 Defining the framework domains

The domains of this model are taken from the VML (Virtual Microdata Laboratory) Security Model. This is a increasingly common framework for defining security as a set of 'safe' characteristics (projects, people, data, settings, and outputs), which are assessed independently and jointly; see Ritchie (2009). This model is employed across the OECD countries; it has been used to define (or has been adopted to describe) RDCs in the US, Mexico, the UK, and Europe; see, for example Wagener [22] on building a social data warehouse, Sullivan [20] for application to the health sector, and Hawkins [10] for the model's role in designing access to tax records. Bujnowska and Museux [8] describe Eurostat's interpretation.

'Safe' in this context is a measure of risk, not a yes-no value. Thus, 'safe data' is the domain in which a particular dataset may pose more or less risk; a specific implementation will embody a level of 'safeness' of the data, which could range from no protection to very high protection.

This is a system model: that is, assessing the 'safety' of data only has meaning in the context of the other domains. Less trust being placed in 'safe people' may be counterbalanced by restrictive IT systems to ensure the same overall level of risk; fewer checks on why or how people are using data may be possible because a stringent disclosure control policy for outputs is in place.

For the purposes of this exercise, the standard domains of projects, people, data, settings, and outputs need some refinement, as shown in Table 1.

[Table 1 about here]

More domains and sub-domains could be added; for example, 'safe outputs' could be broken down into both the number of outputs that are checked and the standards of

checking that are applied; or 'safe settings' could include some system specification such as ISO27001. The above serve for illustrative purposes.

5.2 Defining the criteria/standards

In Table 2, in each of the security domains an illustrative level of protection has been indicated. These are then scored from 0 (implying no protection) to 4 (maximum protection).

[Table 2 about here]

So, to take the top row, a system which does no checks on researchers or projects bar the necessary administrative processes scores 0; a system whereby all projects are read and reviewed by an expert able to critically assess the context of the research gains the maximum score. Moving down, the 'safe data' scores directly reflects the identification possibility. Finally, along the bottom row outputs are scored from 0 (where no checking is done on outputs to see whether they breach confidentiality) to 4 (where nothing is released until it has been scrutinised by trained staff at the NSI).

How does this relate to the principles of access? Consider the 'safe settings (networks)' option. The scores can be rephrased as:

- "There need be no restrictions on where the data can be transferred to"
- "I don't want users to be able to easily share data with the internet"
- "I don't want users to be able to transfer data to outside the network"
- "I want users to work in a restricted area of the network"
- "I want users physically isolated from all other systems"

The table can be refined further. For example, what is meant by 'active training'? In the UK RDCs, this means compulsory attendance at one of the 'safe researcher training'

programmes run by the UK Office for National Statistics (ONS) or the UK Data Archive (UKDA), the UK's main social science data repository at the University of Essex. In fact the criteria could be made quite explicit: Eurostat has agreed [6] the elements of an active training programme designed to meet the 'best practice' level 4 ('safe people (knowledge)' in Table 2), and both ONS and UKDA follow this. However, even the Eurostat manual describes 'what needs to be understood' rather than 'how this is done'. Hence it is possible to refine these criteria substantially without specifying particular implementations.

Note that the scores cannot be directly compared across rows. The VML Security Model is explicitly pluralistic in respect of the safety domains. Hence a score of 4 on one criterion does not make a solution 'safer' than one which scores 3 on another, ceteris paribus.

5.3 Applying the standards

The vagueness in implementation is not an unwillingness to avoid commitment, but essential to the success of the framework. Government organisations tend to be very risk-averse; preferred solutions are therefore, ex ante, ones which have been carried out before or are approved by someone else. With international data sharing, the legal and technical environment is different in every country, and so agreeing on what might be a safe solution is crippled by history from the beginning.

For example, in France until 2011 business data were distributed to licensed users only after an intensive project approval process which included an oral examination of the applicant by a committee in Paris; in the UK, business data were never distributed but access was allowed via secure remote data systems, with checks on project validity limited to confirming the legality of the project. Arguing over which system is 'best' is a dead end: the basis for the implemented solutions is country-specific and arises from past decisions. However, it is clear that both France and the UK can describe their positions in terms of Table 2 and so the differences in perception can be identified within a single framework which aims to be non-

judgmental and so agreeable to both parties. This may seem a small gain, but in terms of getting these organisations to begin discussions, this is a significant leap forward.

Table 3 applies the above criteria to a number of different solutions currently existing. For example, in the first column of figures, the RDC 'VML' operates at level 4 (as defined in Table 2) for checking project validity, but does little to reduce the sensitivity of the data. In contrast, only the data domain is relevant for unrestricted internet resources, and so anonymisation is used to ensure maximum protection inherent in the data. Note that these scores are examples from the author's perspective and do not necessarily reflect the view of the service providers.

[Table 3 about here]

Thus it can be seen that the SDS has stronger incentives for people to act safely (scoring 4 in the 'incentives' sub-domain) compared to the VML (scoring 3). In contrast, the VML has more detailed data (scoring 1)and takes more interest in the non-statistical aspects of the project (scoring 4). The IPUMS solution relies upon the inherent data safety (scoring 3) and on its institutional agreements (scoring 4) to ensure good practice.

This table does not say how 'good' any of the solutions are; it is positive, not normative. For example, IPUMS end-user licence datasets score the same or higher on every criterion compared to the UKDA EUL system. This does *not* mean that IPUMS is 'better' than UKDA, or vice versa; it simply means that IPUMS has decided that a higher level of security meets its objectives (this is not surprising: IPUMS' security model is dominated by the need to meet the standards of the most risk-averse of the 60-plus countries that send it data).

5.4 Designing international agreements using the framework

So far, this conceptual framework identifies how different models solve the security issue, allowing an NSI to start considering which are the domains that are most relevant for the

data release under consideration. Note that a data owner can use multiple channels: in the UK, ONS supplies VML, SDS, IPUMS, and the UKDA with data [13].

The next obvious question is how this can be used actively to design secure systems. For example, Brandt [5] recommended short- and long-term solutions for pan-European data access. As a step on that route, the framework and standards specified here could be the basis for defining three levels of European 'safe centre'; see Table 4 (again, values are illustrative).

[Table 4 about here]

Brandt [6] envisaged using the existing RDC infrastructure but the point of the standards model is that it is infrastructure-independent. If a remote-job model such as Lissy or RADL can meet the requirements, this approach says that it is a valid alternative to an RDC as far as security is concerned. The model looks for functional equivalence, not technical equality.

Problems arise of course when comparisons are not homogeneous. Consider Table 5, illustrating the case of two NSIs looking to deposit data, and three potential hosts; for the moment consider only two domains:

[Table 5 about here]

NSI A would be content with all three solutions for hosting its data. The fact that two out of three exceed its standards is pleasant but does not affect the decision; there could be, for example, cost implications, but these are not relevant here.

NSI B would be willing to place its data in Solution 2, but not Solution 1; but it is not clear if Solution 3 is an acceptable recipient. If NSI B requires that every minimum standard is met, then Solution 3 is not appropriate; if however, NSI B takes an overall view, it might consider that less training but a more restricted IT environment is an acceptable trade-off.

This approach cannot resolve these problems. What it does do is help interested parties to focus on what they want, and whether it can be achieved.

5.5 How extensible is the model?

This model distinguishes between 'systems' and 'networks' in access to data for research. Broadly, a system brings researchers together via a monolithic solution designed, and possibly implemented, by a single authority; this implies ownership and a central architecture, and is how most within-country data solutions operate. In contrast, a network focuses on gateways and communication protocols; what goes on behind those gateways is of no concern to the network.

The focus on the network rather than system characteristics decentralises the decision making process and is designed to encourage innovation in solutions. For example, the world-wide web was developed without the need to change the basic operation of the internet which predated it by two decades. In the principles-based description of data access, not specifying particular solutions should encourage alternatives to be explored.

For example, one area of current interest to data owners is the emerging field of 'cloud computing', buying 'live' computing services from third parties. Beecher and Leclere [3] give an example of using a cloud model to provide access to confidential data. This can be accommodated in the above framework, with data owners being able to delineate the difference between, for example, using cloud services and building their own solution. More importantly perhaps, the argument could be turned on its head: the framework could be used to define the service levels expected by the data owners.

Two other developments suggesting opportunities for data owners are 'grid computing' (using multiple linked computers to carry out major processing tasks in parallel) and distributed storage (where the data files are kept separately and are combined dynamically

at the time of processing). The latter in particular is appealing for international data access, because it suggests the source data can always be stored in the country of origin.

In both these examples, having a common frame of reference is valuable because it allows developers to consider when they might be crossing boundaries between 'acceptable' and 'not acceptable'. In a world of virtual or remote processing, the concept of where data actually 'are' becomes a real issue. This framework can help to identify which are the relevant points of concern. For example, 'the data must be held on our servers' immediately limits discussion; on the other hand, 'I want to be confident the data cannot be accessed from places I have not approved' reflects the underlying objective of the first statement but allows for a range of solutions.

The downside of setting standards is that they themselves can become blocks to progress, however well-intentioned the original plan. This is particularly the case where network protocols cannot be changed without massive expenditure or disruption. By focusing on an abstract level, some of this risk may be avoided, but it is very possible that a framework devised now might be quite unsuitable a few years hence.

Again, this is where the 'specific vagueness' of the standards comes into play. Van den Ende et al. [9] argue that the prospect for adoption of standards is enhanced by being able to adapt to the needs of those who were not part of the original consultation. It is difficult to predict where technology might go in the next few years. On the other hand, "I want users to work in a restricted area of the network that I control" is a flexible, but implementable, criterion.

Technological lock-in is a risk to be managed, and decentralisation can help by providing the incentives for competition. The internet is a positive example: the 1970s protocols, designed for a much simpler world, have been steadily augmented by new ones, driven by the

enormous success of the World-wide Web, in ways which the 1970s designers never envisaged.

6. Issues of implementation

6.1 Is agreement possible and useful?

The framework described above is a simple illustrative model. Assuming, however, that this principles-based model was felt to be a useful way forward, could it be implemented as a set of standard definitions? Sandholtz [19] notes that standards may fail to meet their objectives for two reasons.

First, standards are more likely to be a negative influence if imposed as a directive without relating compliance to operational benefits. Compliance is more likely to be achieved if it saves time or effort, or improves credibility. For example, both the VML and SDS adhere to the disclosure control standards laid down in Brand et al. [6]. Both RDCs already operate a similar standard, but by describing themselves with reference to an independent one they do not need their own statement of operating standards; moreover, they can compare how they operate against other countries who have quite different technical systems. This comes back to the 'signalling' function identified earlier.

Second, the imposition of standards set by 'experts' may cause resistance in other 'experts' who did not contribute to the standards-setting. Although the multi-level approach to standards described here differs from ISO standards studied by Sandholtz, it does seem that the most effective way to kill any development would be to insist on a framework being adhered to.

In other words, effective adoption of the principles-based framework is most likely where it is seen as positive, helpful, low-cost, and (ideally) in tune with the prevailing norms. The point of focusing on the principles of security to build a frame of reference is that agreeing a

framework can be done without any explicit commitment to meet any appropriate standard. This makes it easier, relatively, to get agreement. The multi-level approach to definitions also means that there is less for 'experts' to disagree about: disputes over taxonomy are easier to resolve than evaluating the relative merits of each other's favoured solutions.

For a more detailed exploration in the context of European RDCs and some of the implications for competition and innovation, see [16].

6.2 Paths to development

As noted above, the framework can also serve as a way of specifying standards to be achieved when designing new systems. One possible three-stage development route then is

1. **Definition**: a principles-based reference framework is defined
2. **Retrospective adoption**: data owners/infrastructure providers begin using the framework to describe their systems
3. **Prospective adoption**: the framework is used as a design criterion:
    a. Data owners begin using the framework to define their requirements
    b. Infrastructure builders begin using the framework to define their systems

Most importantly, each of these stages is voluntary. Countries do not need to agree to the definition, or evaluate their own solutions. Use of the framework is a positive decision: because it is better than the alternative.

This approach by itself does not solve all the issues of international data sharing; it is meant as part of a suite of methods for separating complex issues into more digestible fragments.For example, it has nothing to say about the legality of data sharing; this is not the purpose. The point of the framework is to agree the rules of engagement, with each

country being left to decide how its strategic aims can be met within its own legal structures. Only the point of connection matters; how that connection is achieved is up to each country.

Van den Ende et al. [9] note that there is a time-dependency in the development of successful standards: early movers may generate 'co-evolutionary' responses in other participants. This has been the case in within-country data security: the VML Security Model described earlier was developed for ONS in 2003 but has since spread across several countries and into Eurostat publications. The apparent conformity of terminology has encouraged the wider adoption of the model into the data security literature.

7. Summary and thoughts on future development

NSIs take decisions on whether to invest in research infrastructure on the basis of cost, benefits and the security risks involved. The principles-based framework is designed to take the latter out of the equation, by making clear that all levels of security are available, albeit it at different cost. The framework is implementation-independent by design, and it requires NSIs to focus on what they want, rather than how the aim is achieved.

The framework defined above is necessarily basic. Even if the framework were agreed as it stands there are many refinements needed. For example, 'active training' is marked as giving the most security, but what does this consist of? Should there be an exam and certification? Do all countries want the same training? How active is 'active'? On outputs, is automatic checking of all outputs safer than manual checking of only some? Most importantly, can a linear model be devised – should there be, for example, several different ways of scoring top marks in a domain?

Nevertheless, even in outline this approach may help to break through the tangled concepts of international data access, by separating out the security components which are important from those which are not.

Just as important as the concept is the scope for agreement. Countries are more likely to support a framework which focuses on effective taxonomy, rather than one which seeks to impose an implementation standard. The lack of reference to favoured methods or technology, and the explicit recognition that a variety of approaches have value in achieving access outcomes, makes acceptance easier. Even the long term aim, of such an approach being used to specify acceptable implementations, assumes that countries will want to do this because they find it beneficial, not because it is required.

From the NSI's internal perspective, the framework can also bring gains. Descriptions of what an NSI's security policy aims to achieve are easier to align with corporate goals, compared to a more implementation-specific viewpoint. For example, ONS' Data Access Policy, adopted in 2011, follows the VML Security Model exactly and uses the above criteria to describe all its data access options in one setting.In addition, setting security goals in terms of standards allows for multiple implementations to be covered by the same corporate policy, and for those implementations to be changed as the situation arises without the need to change the policy.This was done in 2011 when the Security Data Service became a third-party provider of data services to ONS.

As noted, this standards-based approach only addresses the networkneeds for international data sharing, and ignores local considerations, such as particular legal structures. Also, the standard is necessarily voluntary. Hence, the vision of international data sharing discussing focusing solely on principles may be unrealisable.

Is the journey then worth it? This paper argues that it is, for three reasons.

- A common way of describing disparate solutions has merit in itself. For example, the multiple access paths in ONS' 'data access spectrum' [13] can all be placed in the

above framework, allowing one to easily see where the differences between options arise.

- The framework focuses on the principles of security, rather than the technology. A key recent development has been the recognition that security is an outcome, not a constraint. This framework makes that focus explicit.
- The history of networks from the organisational literature shows that clear, effective standards are essential for their use and development; and that standards encourage innovation by lowering the cost of connecting to the network. There are many uncertainties about the development of technology, as well as approaches to risk; clarifying the network gateways allows innovation to flourish without needing to redesign systems.

Overall, these suggest that the journey may be worth the effort even if the ultimate end is unattainable. This is a long-term proposal; even if the above framework were accepted now as it stood – which would require a sea-change in NSI perspectives – the move from retrospective to prospective adoption is likely to take some years. Moreover, the shift from implementation to objectives may have unexpected effects. For example, a natural implication of this approach is a stronger case for the outsourcing of data management, as organisational objections (unwillingness to consider alternative hosts because "we can't trust others") are explicitly being challenged.

At present, international data sharing is a long way from any prospect of general arrangement or approach. However, over the last ten years access to microdata within many countries has changed beyond recognition – both in technology and in the approaches to risk and security. The similarity with debates over international data sharing is clear; the issues being raised in cross-country data sharing are akin to those raised within countries over the last decade, and which have now been addressed. Will there be a similar shift in

international data sharing? It is not possible to say, but this paper has tried to suggest a way in which the discussion may be usefully taken forward.

Acknowledgements

This paper is based on presentations given to the 3rd Workshop on Data Access and the International Association of Social Science Information Services and Technology conference (IASSIST-2010), as well as submissions made as part of Brandt [5] with Richard Welpton of the UK Secure Data Service. I am grateful to workshop and conference participants, to Don Webber at University of the West of England, Bristol, and to three anonymous referees for helpful comments.

References

[1] N. Ahmad, *OECD Conference on, and feasibility study of, microdata,* briefing paper STD/CSTAT/RD(2006)2, OECD. http://www.oecd.org/std/37502925.pdf

[2] A. Airaksinen, A. de Panizza, E. Bartelsman, E. Hagsten, G. van Leeuwen, M. Franklin, M. Maliranta, P. Kotnik, P. Stam, P. Rouvinen,S. Farooqui, S. Quantin, S. Svanberg, T. Clayton and Y. Barbesol, *Information Society: ICT impact assessment by linking data from different sources; Final Report,* Eurostat , 2008. http://epp.eurostat.ec.europa.eu/portal/page/portal/information_society/documents/Tab/ICT_IMPACTS_FINAL_REPORT_V2.pdf

[3] B. Beecher and F. Leclere, *Exploring new methods for protecting and distributing confidential research data,* Presentation to Coalition for Networked Information Membership Meeting Fall 2009, 2010. http://www.slideshare.net/bryanbeecher/exploring-new-methods-for-protecting-and-distributing-confidential-research-data

[4] S. Bender and J. Heining, *The Research-Data-Centre in Research-Data-Centre Approach: A First Step Towards Decentralised International Data Sharing,* presentation to IASSIST-2011, Vancouver, June, 2011. http://www.iassistdata.org/downloads/2011/2011_e2_bender_etal.pdf

[5] M. Brandt. *Decentralised Access to EU-Microdata Sets,* final report to Eurostat on grant agreement no. 61102.2008.001-2008.828, Eurostat, 2010. http://www.cros-portal.eu/sites/default/files//Final%20report%20DA.pdf

[6] M. Brandt, L. Franconi, C. Guerke, A. Hundepool, M. Lucarelli, J. Mol, F. Ritchie, G. Seri and R. Welpton, *Guidelines for the checking of output based on microdata research,* final report of ESSnet sub-group on output SDC, Eurostat, 2010. http://neon.vb.cbs.nl/casc/ESSnet/guidelines_on_outputchecking.pdf

[7] N. Brunsson, A. Rasche, and D. Seidl, The dynamics of standardization: three perspectives on standards in organizational studies, *Organization Studies* **33** (2012) 613-623, doi:10.1177/0170840612450120. http://oss.sagepub.com/content/33/5-6/613.full.pdf+html

[8] A. Bujnowska and J.M. Museux, *The Future of Access to European Confidential Data for Scientific Purposes,* Work session on Statistical Data Confidentiality 2011, Eurostat, 2012 http://www.unece.org/fileadmin/DAM/stats/documents/ece/ces/ge.46/2011/43_Eurostat.pdf

[9] J. van den Ende, G. van de Kaa, S. den Uijl, and H.J. de Vries, The Paradox of Standard Flexibility: The Effects of Co-evolution between Standard and Interorganizational Network".*Organization Studies* **33** (2012), 705-736, doi:10.1177/0170840612443625 http://oss.sagepub.com/content/33/5-6/705.full.pdf+html

[10]M. Hawkins , *The HMRC data lab,* presentation to KAI International Conference on Taxation Analysis & Research, 2 Dec 2011. http://www.esrc.ac.uk/hmrc/images/Session%2012%20The%20HMRC%20Datalab_tcm19-19599.ppt

[11]T. Kruten,.*A remote access solution: The Lissy System at LIS Asbl,* presentation to Eurostat Workshop on Microdata Access, Luxembourg, 3-4 December 2008. http://epp.eurostat.ec.europa.eu/portal/page/portal/research_methodology/documents/7_2_LIS.pdf

[12]R. McCaa, S. Ruggles, M. Sobek and W. Thomas, *IPUMS-International: Free, Worldwide Microdata Access Now for Censuses of 62 Countries--80 by 2015,* paper for 58th International Statistical Institutes conference, Dublin 21-26 August, 2011

http://www.hist.umn.edu/~rmccaa/sts065_ipums_international_future_microdata_access.pdf

[13]F. Ritchie, UK Release Practices for Official Microdata, *Stat. J. of the IAOS* **26** (2009), 103-111. http://iospress.metapress.com/content/08km250w1n536w85/?p=db53a55c3325436c89c4632a67edc846&pi=6

[14]F. Ritchie, *Risk assessment for research access to confidential microdata,* presentation to John Deutsch Institute conference on access to business data, March; and 3rd Workshop on Data Access, May, 2010. http://www.felixritchie.co.uk/publications/wda_risks_v1.ppt

[15]F. Ritchie, *Methods for analytical access to confidential data.* Paper prepared for OECD Microdata Working Group, OECD, 2011.

[16]F. Ritchie, *Access to sensitive data: satisfying objectives rather than constraints.*Cardiff:WISERD Data Resources Working Paper no.7, 2012. http://www.wiserd.ac.uk/wp-content/uploads/2012/02/WISERD_WDR_007.pdf

[17]F. Ritchie and R. Welpton, *Access without boundaries*, IASSIST-2011 presentation, 2011.

[18]F. Ritchie and R. Welpton, *Sharing risks, sharing benefits: Data as a public good*, Worksession on Statistical Data Confidentiality 2011,Eurostat, 2012. http://www.unece.org/fileadmin/DAM/stats/documents/ece/ces/ge.46/2011/presentations/21_Ritchie-Welpton.pdf

[19]K. Sandholtz, Making Standards Stick: A Theory of Coupled vs. Decoupled Compliance, *Organization Studies* **33** (2012), 655-679, doi:10.1177/0170840612443623. http://oss.sagepub.com/content/33/5-6/655.full.pdf+html

[20]F. Sullivan, *The Scottish Health Informatics Programme*, presentation to Health Statistics User Group, 2011. http://www.rss.org.uk/uploadedfiles/userfiles/files/Frank-Sullivan-linkage.ppt

[21]D. Trewin, A. Andersen, T. Beridze, L. Biggeri, I. Fellegi, and T. Toczynski, *Managing statistical confidentiality and microdata access: Principles and guidelines of good practice*, final report for UNECE/CES, 2007.

[22]R. Wagener, *Microdata and Evaluation of Social Policies,* paper prepared for the colloquium "En route vers Lisbon", Public Policy Research Centre Henri Tudor, , December, 2008. http://webserver.tudor.lu/cms/lu2020/publishing.nsf/0/FDECF548D12BC30BC12575140048AB73/$file/16h15_Raymond_WAGENER.pdf

Table 1 Domains of risk in the extended 'VML Security Model'

Domain	Subcategory	Meaning
Safe project	-	Project meets legal/ethical/process requirements
Safe people	Knowledge	Researchers have sufficient knowledge to use data safely
	Incentives	Researchers have sufficient incentives to use data safely
Safe data	-	There is protection in the data themselves
Safe settings	Access	Connection to the data is secure
	Networks	Opportunity to move data to other networks/media is limited
Safe outputs	-	Statistical outputs are checked to ensure no accidental breaches of confidentiality

Table 2 Illustrative standards for desirable criteria

Safe…	**← No protection**				**Strong protection →**
score:	**0**	**1**	**2**	**3**	**4**
Projects	Administrative processes only (eg name and address for contact purposes)	Check researcher background	Check use is for statistical purpose	Review by support officers able to critically assess feasibility and need for data	Review by support officers able to critically assess impact of research
People (knowledge)	Administrative processes only	Check researcher background	Written assent to conditions of access	Passive training	Active training
People (incentives)	No effective sanctions	Procedural sanctions only	Mix of civil, criminal or procedural sanctions	Civil, criminal and procedural sanctions	Civil, criminal, procedural and institutional sanctions
Data	No data protection	Removal of direct identifiers	Identification within controlled environment unlikely	Identification outside controlled environment unlikely without sustained effort	Identification outside controlled environment not possible without exceptional effort/luck
Settings (Access)	No restrictions	Access only from limited sites with no supervision	Access from secure networks with no supervision	Access from secure networks with occasional supervision	Access from secure networks with continual supervision
Settings (Networks)	No restrictions on data transfer	No internet access	No internet, local/mobile storage or printers	No access to other parts of network or mobile storage	No network connection, no mobile storage
Outputs	No checks	Random checks	Random plus targeted partial checking	Full checking except for 'experienced' researchers	Full checking

Table 3 Applying the standards for specific systems: illustrative scores

Unit	**VML**	**SDS**	**RADL**	**LISSY**	**IPUMS**	**UKDA**	**Internet**
Type	**RDC**	**RDC**	**RJS**	**RJS**	**EUL**	**EUL**	
Safe…							
Projects	4	3	3	3	3	0	0
People (knowledge)	4	4	2	2	2	1	0
People (incentives)	3	4	2	2	4	2	0
Data	1	2	3	3	3	3	4
Settings (access)	3	2	1	1	0	0	0
Settings (networks)	3	3	4	4	0	0	0
Outputs	4	4	1	3	0	0	0

Explanatory notes

Unit:

- VML=ONS Virtual Microdata Laboratory, UK
- SDS=Secure Data Service at the UKDA, UK
- RADL=Remote Access Data Laboratory, Aus/NZ
- Lissy=earnings data, UK/Luxembourg
- IPUMS=anonymised international Census microdata, hosted in US

Type:

- RDC=research data centre
- RJS=remote job server
- EUL=End User Licence

Note: scores are illustrative based on the author's own perception

Table 4 Specific standards for European-accredited secure RDCs: illustrative scores

	'minimum'	**'best practice'**	**'maximum security'**
Safe…			
Projects	2	3	4
People (knowledge)	3	4	4
People (incentives)	3	4	4
Data	3	1	1
Settings (access)	3	3	4
Settings (networks)	3	3	3
Outputs	3	3	4

Note: scores are illustrative based on the author's own perception

Table 5 Example of unresolved security preference

	NSI wants…		**Potential homes…**		
	NSI A	NSI B	Solution 1	Solution 2	Solution 3
Safe people	3	4	3	4	3
Safe setting	3	3	3	3	4