**Working Paper**
ENGLISH ONLY

**UNITED NATIONS ECONOMIC COMMISSION FOR EUROPE (UNECE)**

**CONFERENCE OF EUROPEAN STATISTICIANS**

**EUROPEAN COMMISSION**

**STATISTICAL OFFICE OF THE EUROPEAN UNION (EUROSTAT)**

**Joint UNECE/Eurostat work session on statistical data confidentiality**
(Helsinki, Finland, 5 to 7 October 2015)

Topic (iv): Access to Statistical Data for Scientific Purposes

# Micro, remote, safe settings (safePODS) – extending a safe setting network across a country

Chris Dibben [*]

[*] Director, Administrative Data Research Centre – Scotland and School of Geosciences, University of Edinburgh, Edinburgh, Scotland, UK. chris.dibben@ed.ac.uk

## 1 Introduction

The Administrative Data Research Network (ADRN) is a UK-wide partnership between universities, government departments and agencies, national statistics authorities, the third sector, funders and researchers funded by the UK's Economic and Social Science Research Council. It aids accredited researchers carry out social and economic research using linked, de-identified administrative data, ensuring that the risk of data being re-identified is minimised through strict governance and structural controls. As part of the governance and structural control over the research process, the network provides secure environments for the researcher to work in. Data and output cannot be taken out of this safe setting by a researcher. Output for publication are only released through the centre after statistical disclosure control. At present there are 6 research centres with safe settings across the UK. This is a limitation because it requires many researchers to travel, sometimes quite long distances to access data. The ADRN is therefore looking at expanding its network of safe settings. However a safe setting can be costly to set up, as it involves the building or modification of a room. In some cases safe settings can also be resource intensive to manage for local institutions. This may mean institutions are unwilling to create a safe setting and the fact that they are not controlled by the network can be an added risk. A new concept which overcomes some of these barriers, is the development of prefabricated micro, safe-rooms which can provide for a fully controlled and consistent environment for data analysis. Importantly this control can be from a geographically distant location away from the hosting institutions. In this paper I will outline the concept, design and results from a pro-type study located in a university library.

## 2 Linked administrative data

The joining of data records corresponding to the same individual (or sometimes organisations) across multiple datasets is increasingly a required function of research service infrastructures. Through this process, new data structures are built; potentially powerful ones that can facilitate important lines of enquiry within multiple research areas. In many instances, the size of these databases makes it impractical to seek active consent from individuals and therefore the data being manipulated in the linkage process is of a special character, where there is an extremely strong need (legally and ethically) to ensure that there is no disclosure of information to any party about individuals within the datasets. Working with data that is strictly non-personal (i.e. absolutely anonymous) guarantees that protection, but is rarely achievable in a data linkage context and indeed may actually be impossible with any useful data (Ohm 2010). Instead, what is required is the construction of a 'data environment' in which the process of re-identification is made so unlikely that the data can be judged as *functionally anonymous*. This type of environment is formed through the security infrastructure and governance processes that shape the behaviour of those accessing the data; and the data linkage and analysis models that structure the operational processes.

## 3 The production of functionally anonymous data

The environment within which data can be argued to be functionally anonymous is typically constructed through multiple elements. In the UK these sets of elements have been described as the 'five safes', that is: safe projects, safe people, safe data, safe outputs and safe environments. If these all exist in concert at the same time and place then the argument can be made that the data is, within reasonable bounds, in practise anonymous.

Safe projects and safe data are typically produced through independent scrutiny of a project proposal and a set of rules or guidelines around the nature of the data that balances privacy against utility. Though this process reduces the risk of unintentional disclosure of information associated with an individual, it does not make the intentional gaining of this information impossible. The possibility that an individual attempts to gain information is instead tackled though the production of a 'regulated space'. That is the space in which the data exists, is (firstly) only accessible to individuals who are felt to be very unlikely, due to character, professional position and training, to attempt to gain this information and (secondly) allows an 'unequal gaze' to exist, where there is the constant *possibility* of observation (Foucault, 1977). This possibility of observation and the resulting risk of some form of sanction or punishment reinforcing a form of self-discipline within which the risk of an attempt at gaining the information is substantially reduced. In concert then these elements combine to produce a situated state within which the risk of a disclosure of personal information is suitably small.

This situated state is typically achieved within a research structure like the one presented in figure 1. In this the various parts of the processing of the data are separated, part of the process of producing safe data whilst minimising the loss of research utility. This separation of function is particularly helpful in reducing the risk to privacy when linking administrative datasets via a probabilistic matching process on personal identifiers (eg name, address, data of birth etc.). A need that commonly exists in countries where there is not a universal identification code. In this case the use of *separate* parties to carry out the matching and provide the secure access to the data means that there is no need for the *identifying* information and the *information* on the that person to exist in a single place at the same time (ie part of 'safe data'). The other 'safe' elements are then instituted by the research centre and the bodies offering oversight to it. A very important aspect of this is the point of access to the data provided to researchers – often described as the safe setting.

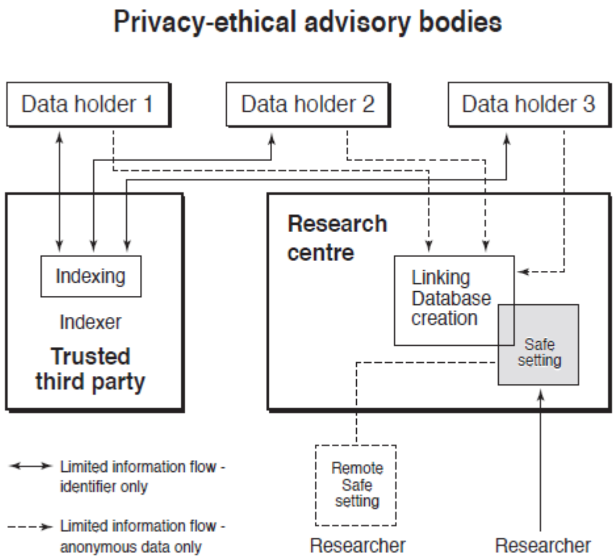


**Fig 3.1** Informational flows in a typical 'separation of functions' approach to data linkage.

## 4 Safe settings, shaping behaviour and producing regulated spaces

The core goal of a safe setting is a shaping of behaviour that then allows a strong claim that the data is functionally anonymous to be made. In other words that there is a sufficiently small risk of any attempt to re-identify individuals and information associated with them in the data and that any risk of unintentional re-identification is also suitably small.

As has been discussed in section 3 a key part of this shaping of behaviour is through the design of a safe setting, its rules and the observation of individuals in the space. So for example a policy of sanctions around the misuse of data requires researchers to be 'observed' in their processing of the data in order for inappropriate behaviour to be identified or importantly potentially identified. Although the reasonable assumption (given other aspects of the 'safe' approach) is that none of the users are likely to act inappropriately (eg given their training, professional position etc.).

Typically the safe setting is physically located within the research centre that is managing the data linkage/ research process. Though this may be convenient for the research centre staff, it may be very inconvenient for researchers who may want to access the data. If they are located some distance from the research centre, given the amount of time that may be required in making administrative data research ready, distance may become a strong disincentive to use. This may be a threat to the entire administrative data research endeavour as the research structure outlined above is necessarily expensive and therefore a high use of the resource is needed to justify the expenditure.

There is, as a result, frequently a need to produce some form of access remote to the research centre in order to ensure the long term financial sustainability of the research infrastructure. However, given the intrinsic nature of a safe setting, the requirement of remoteness from the research centre potentially threatens to destabilise the regulated space of the safe setting. Specifically it may weaken the 'gaze' of research centre and therefore the researcher self-regulation, one of the core aspects of the argument that the data remains functionally anonymous. The challenge is therefore to design a form of remote access or a remote safe setting that reproduces, as effectively the regulated space of the safe setting but remote from the research centre.

A successful remote safe setting then needs to replicate the conditions present in the research centre. Though this may be possible through purpose built rooms in institutions, it may be difficult and expensive to achieve. It may for example be difficult in an institution with a relatively low number of researchers to build a use case to support the investment and the loss of space associated a purpose built safe room. Existing facilities that could be used will not necessarily reflect the perhaps tighter control managed in a purpose built research centre.

It should be noted in passing that the provision of 'synthetic data' would be another method for making the data in some sense accessible, remote from the research centre (Rubin, 1993).

## 5 Remote micro safe settings

Remote micro safe settings or safePODs are a proposed solution to this problem. They aim to replicate the research centre safe setting but remote from it.
In order to assess whether this is possible, it is necessary to identify what is needed in a safe setting and examine whether this can be replicated in a remote micro safe setting. If the essence of a safe setting holding a terminal (ie thin client) to access a remote data holding (ie no actual data is contained in the workspace) is deconstructed, it might be argued that the following conditions are required:

1. Controlled access (ie it is not in a public space) to the space housing the work space.
2. Methods for controlling who has access to or is in the work space.
3. Methods for monitoring behaviour in the workspace – the 'gaze' of the research centre.

4. That the remotely executed work is only visible to those in the work space.
5. A pleasant working environment that discourages any forbidden behaviour.
6. Strong environmental ‘cues’ that encourage safe behaviour.
7. A built structure that needs to resist a deliberate but not a determined malicious intruder (eg an intruder using considerable force or tools).

In our examinations of these conditions, we have concluded that a 'prefab' micro safe setting that could be fully specified centrally and then located in institutions could be fully compliant with the above conditions. Indeed it might be easier to fully realise these conditions in a purpose built micro safe setting than in a typical ‘converted room’ type safe setting.

There would seem to be major advantages with this approach over, for example, accrediting rooms converted in an institution.

1. The safe setting design/ environment would be identical across a network and the safe setting network, as a regulated space, would be more consistent
2. Could be design to maximise the dual aims of a safe setting: safe and secure but convenient and comfortable research environment.
3. This would be a scalable and so a more affordable solution for small institutions – larger institutions could simply have multiple units
4. Could be designed so de- and reconstruction was possible and therefore rhw units moved within the country if not used sufficiently or within an institution when restructuring.
5. Could be reusable as simple workstations/ quiet work places if there use became redundant overtime.

There will be some disadvantages over a converted room:

1. It will not be as space efficient for multiple users ie you could fit more people in an open lab.

The security of any form of remote safe setting will of course depend on the method of distant access. This is typically achieved with some form of secure encrypted Virtual Private Network technology with strong user authentication. As this is common to any type of remote safe setting we will not discuss this further. However one form of vulnerability that is more specific to the design of the safe setting is the potential vulnerability of computer equipment emissions. These in particular circumstances can be interpreted (Kuhn and Anderson 1998). This is a rather low threat, with some possibility of reconstructing what is being seen on a monitor screen. This possibility will be dependent on a number of factors, such as the existing shielding of the computer, the build materials and how close an ‘attacker’ could get to the safe setting. As this type of activity requires an ‘attacker’ to set up rather extensive equipment near a safe setting, general security in the building housing the safe setting will be a defence. Safe setting electrical equipment could additionally incorporate conductive shielding, shielded external cables and the provision of additional filters in interfaces and power supply lines. The NATO ‘TEMPEST’ specification describes emission test requirements for three different security levels based on how close the attacker can get to their targeted equipment. Any decision to provide additional shielding in the safe setting should balance such cost with a realistic assessment of an attack and the implications of a loss of data, however the prefabricated remote safe setting concept would allow this type of protecting to be built into the design.

## 6 'SafePODS'

Between 2014 and 2015 the Administrative Data Research Centre – Scotland developed a prototype micro remote safe setting – described as a safePOD and installed it within a university Library (figure 6.1). The funding for this was provided by the ESRC.

Figure 6.1 SafePOD external and internal view.

The safePOD measures approximately 2m x 2m x 2m and is designed to accommodate one person, though two could use the unit. It does not hold any data but accommodates a thin client that can link, provided two factor authentication is provided, to a researcher's remote workspace via a secure connection to an individual Administrative Data Research Centre. Only the researcher is able to see the screen from within the Pod. Inside the safePOD there are typical office furniture including a height adjustable desk, chair and monitor. There is flexible ventilation options and dimmable lighting. The safePOD is designed to accessible for wheelchair users and not only include an intruder alarm but also an emergency alarm in case anyone needs assistance.

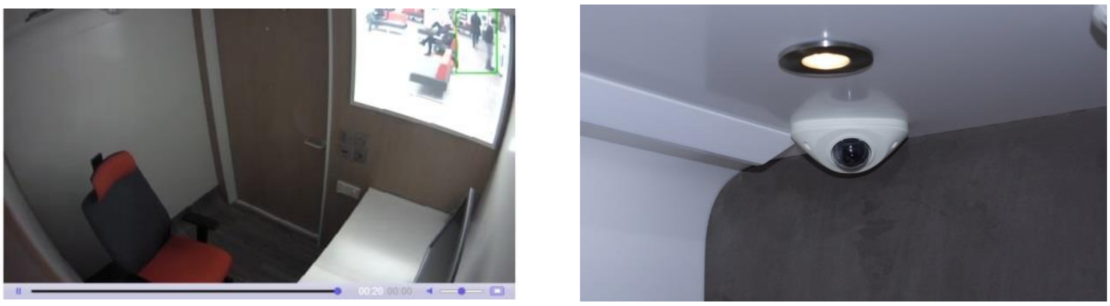

Figure 6.2 The CCTV camera monitors and records activity remotely.  Alerts are sent on motion activation.

The safePOD has a CCTV monitoring system that has person and motion detection capabilities (figure 6.2). Entrance to the POD is controlled through a remote biometric database, with the research centre able to timetable access (ie to particular accredited researchers – whose accreditation is authenticated by this biometric information) access during specific dates and times (ie only the specific researcher's finger print will open the door during that period) (figure 6.3). There is however an emergency over ride key available to the local institution. This means that all aspects of the safePOD management can be managed remotely (eg scheduled cleaning, researcher booking etc.). The CCTV, management of user access to the remote server and biometric system can therefore be used together to both monitor and control behaviour in the safePOD (eg a session can be ended if any inappropriate behaviour is suspected).

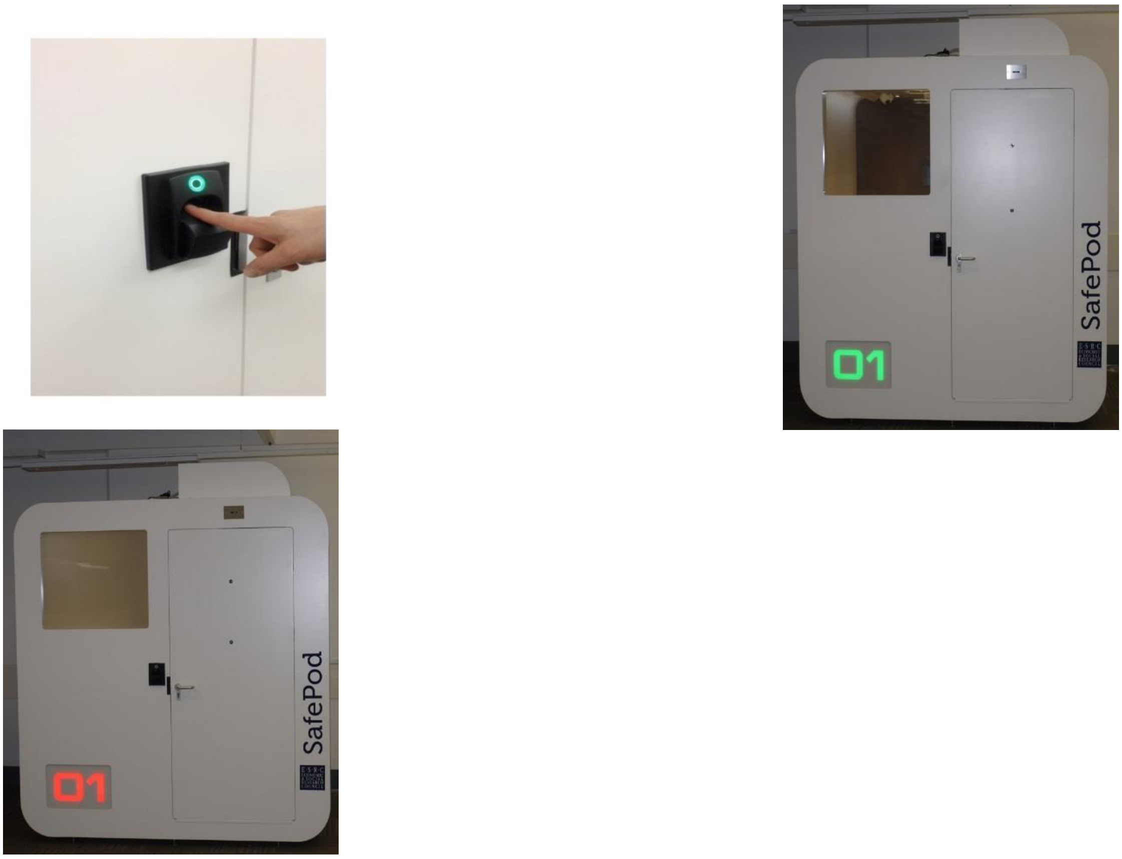


Figure 6.3 Biometric finger print entry

We expect the safePOD to have a unit cost to be around £20,000.

## 7 Conclusion

The safePOD concept therefore represents a flexible tool for extending a safe setting network beyond a research centre but arguably with very little increased risk in the potential of a disclosure of personal data. It involves relatively little management by the host institution and so unlike the conversion of a room into a safe setting may be relatively easier for a local researcher to organise. It may also have particular advantages over traditional 'safe lab' type safe settings where researchers for example can potentially look, rather easily, at the data on another's monitor screen. Indeed with the features instituted it is possible that the safePOD may actually have a greater degree of control and institute a greater level of self-discipline in users than other types of safe setting.

## References

Foucault, Michel. *Discipline and punish: The birth of the prison*. Vintage, 1977.

Kuhn M and Anderson RJ, 'Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations', in David Aucsmith (Ed.): *Information Hiding, Second International Workshop, IH'98, Portland, Oregon, USA, April 15-17, 1998, Proceedings, LNCS 1525*, Springer-Verlag, pp. 124-142, ISBN 3-540-65386-4.

Ohm, P. (2010) 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymisation', UCLA Law Review, Vol. 57, p. 1701, 2010

Rubin, D. B. (1993). Statistical disclosure limitation. *Journal of official Statistics*, *9*(2), 461-468.