University of the West of England BRISTOL

Faculty of Business and Law

Addressing the human factor in data access: incentive compatibility, legitimacy and cost-effectiveness in public data resources

Felix Ritchie
University of the West of England, Bristol

and

Richard Welpton
University of Essex

Economics Working Paper Series
1413

University of the West of England BRISTOL

bettertogether

Addressing the human factor in data access

Incentive compatibility, legitimacy and cost-effectiveness in public data resources

Felix Ritchie, University of West of England, Bristol

Richard Welpton, University of Essex

Abstract

Traditional models of incentivising people suggest that positive incentives are more effective than negative ones. We argue that in data access the opposite can be true, as the assumptions made at the design stage can fundamentally change the user environment and hence perceptions of the 'right' way to act. Such assumptions also affect the 'legitimacy' of any control measures: empathy can encourage positive reinforcement. Both of these issues are dependent upon the training given to data users, particularly if this can develop a self-policing ethos. Hence training (of the 'right kind') should be seen as a positive investment to improve the benefit:cost ratio, rather than unavoidable expenditure.

The focus on policing rather than engagement is particularly acute when considering the vast research potential of the data resources in the public sector. Although evidence-based policymaking is widely supported, specific costs and diffuse benefits encourage an overly risk-averse environment amongst the data owners. Discussions about user risk are dominated by academic studies based on worst-case scenario planning.

This study uses an example of research data access to demonstrate how insights from criminology, psychology and economics, supported by evidence rather than theory, can provide substantial improvements in the risk profile, the user experience and the net cost of data access. The example also demonstrates how an effective culture of data security can be developed using the carrot rather than the stick. While the example reflects a particular environment, the lessons that can be drawn from this are more general. In particular, we suggest ways that the perception of cybersecurity experts, that people are the weak link in any security system, can be turned into a potential positive benefit.

1. Introduction

Much of the data collected by private and public sector bodies is confidential personal data; that is, use and re-distribution of that data is subject to legal controls to ensure that the risk of unauthorised access to the data is minimised.

Making appropriate use of the data requires managing risks in multiple dimensions. Desai et al. (2014) suggest breaking the problem into five questions:

- safe projects: is the use lawful/proper?
- safe people: can the users be trusted?
- safe settings: does the access method provide some security?
- safe data: has the data some inherent protection, eg via anonymisation?
- safe outputs: are the products of such analysis suitable for wider distribution?

These ‘five safes’ can be used to simplify the decisions into a set of linked sub-problems, each amenable to specialist input.

Different professions have different interests. The legal profession and privacy campaigners tend to focus on ‘safe projects’, the appropriate use of data. Technical specialists may concentrate on reducing the risk of a leak from an inappropriately-secured IT system. However, in many – perhaps most – cases, the human factor is the most important. For example, IT systems are often hardened against cyber-attack, but there may be little that can be done to stop employees of an organisation copying data onto memory sticks. Similarly, it is crystal clear that members of the tax department should not pass on details of celebrity earnings to the newspapers – and yet it happens.

This human factor is typically controlled by what may be termed the ‘policing’ approach: inform users of legitimate uses, the penalties of misuse, and check for compliance. This paternalistic approach is appealing to the data controllers: it is straightforward to show that sufficient information has been provided, and makes clear that any misuse derives from the actions of the user, against the explicit instructions of the data controller. If misuse occurs, then the clear response is that the information sharing or enforcement is ineffective and needs to be strengthened. This lack of ambiguity over who must do what is also appealing to managers, lawyers and mainstream economists: in all cases, giving clear, easily-understood advice addresses the human factor – and if it does not, the blame clearly lies with the human.

This perspective contradicts evidence from criminology, behavioural psychology and heterodox economics that the paternalistic ‘us and them’ approach fundamentally misunderstands human nature. It also ignores one of the most persistent findings from game theory and experimental economics: that co-operative solutions nearly always outperform antagonistic or autocratic approaches, both for society as a whole and the individuals involved.

This paper looks at how behavioural insights can be used to improve both the efficiency and security of confidential data use. It takes the specific example of research use of government data. This is because in this field it is easy to identify the ‘policing’ perspective in action, the reason why that is seen as a rational decision, and the financial and operational consequences of such a perspective. In other sectors, for example supermarket loyalty cards, the commercial incentives are different. Nevertheless, the insights from the specific example have a wider application, in terms of suggesting how a better (and more evidence-based) understanding of human nature can improve data security.

The next section introduces the specific example, of how governments typically make data available for research use, and the imperatives that drive their decision-making. Section 3 considers the 'rational' model of policing and why it appeals, and the evidence base. Section 4 then revisits the assumptions of the policing model, discussing more recent theories based upon human behaviour. Section 5 applies the model to two cases of research data access (a controlled facility and a distributed data file), and reviews the cost/security effectiveness of this alternative approach. Section 6 concludes with a discussion of the wider lessons that can be drawn.

2. Research use of confidential government data

Governments acquire vast amounts of information on legal and natural persons, through administrative sources (such as tax records) or targeted data collection (such as a Census or a survey of manufacturing companies). Some of this information is highly sensitive (medical records), some is not (registered address of a business). While some is in the public domain (court judgements), most of the data is acquired under either an explicit or implicit promise of confidentiality.

Governments are under pressure to increase the use of this data. There are three drivers for this

- Evidence-based policymaking, increasingly seen as an essential part of good governance; this usually means quantitative analysis of policy proposals
- Cost pressures on statistical organisations to find ways to replace statistical data collection (such as surveys) with non-statistical sources (such as administrative records)
- Improved technological and statistical techniques allowing datasets to be linked and analysed jointly, increasing the range of questions that can be answered

Taken together, these three have led to the widely-held belief that using government data only for its original purpose (charging tax, or producing statistics on employment, for example) ignores the potential for more analysis at negligible additional cost; see eg Desai (2012). In managerial terms, the investment in data collection could be 'leveraged' much more effectively.

This increased use of data occurs through two channels. Government departments may make use of this it themselves; or they may make it available to third parties, either under contract (where the analysis is for their purposes) or for general research not directed by the department. In the latter cases, data may be released through distribution of the source data (over the internet or on CD, for example) or distribution of access (for example, through the provision of analytical tools or through controlled research facilities). In all cases, data are anonymised to a level consistent with other controls on the data such as licensing arrangements. The data controllers are responsible for devising and implementing strategies to manage those risks.

A problem for government bodies is that they are often not the beneficiaries of the secondary analysis of their data. For example, if the Social Security department makes its benefits data available to academic researchers, this may lead to many research articles; but it is difficult to quantify the 'value' of such research to the social security department. As Ritchie and Welpton (2012) discuss, research access to data is typically a pure public good where the data controller is unable to capture the gain to society, and so is likely to under-provide access. In addition, the data controller has little incentive to invest in understanding the uses of the data.

Even where the government department has an interest in the data use, it may be limited in its ability to exploit the data. For example, an energy department may want to understand the power generation market more clearly. This requires both expertise and resources, which may not be available within the department. A common solution is to commission outside experts (in academia or consultancy) to provide the analysis. This use of outside expertise as and when necessary can be very cost-effective, but once again it creates a barrier between the data controller and the data user.

In short, government management of data assets can often be characterised as providing a service which provides a risk to the data controller without necessarily providing a clear benefit. This is the model of 'specific cost' (to the data controller) and 'diffuse benefit' (to society as a whole) which public sector governance studies have argued leads to under provision of key services (Ritchie, 2014).

An additional complication is that popular perceptions of government often focus on negative aspects: good practices are not noted, whereas mistakes are highlighted and attributed to the general ineffectiveness of 'government' (OACG, 1998; Lofstedt, 2004; Moore, 2010). Sometimes perceptions are based on fact but often the complexity of privacy issues leads to simplistic and inaccurate messages in popular media with an overwhelmingly negative portrayal of government competence (Bhatta, 2003)

These three factors (limited benefit, limited resources, and concern over public perceptions of error) encourage a risk-averse stance amongst government data controllers (Ritchie and Welpton, 2012; Ritchie, 2014)[1].

In considering research access to government data, this risk aversion is given a theoretical justification by the worst-case scenario planning which dominates the academic literature. Almost all papers in statistical disclosure control (SDC: ensuring that tables, microdatasets or other statistical products do not allow individuals to be identified and targeted) focus on the concept of an 'intruder'. An intruder is an individual whose primary intention is to breach SDC protection, and who is prepared to devote resources and expertise to that end. In many cases, the resources available to the intruder are considerable: a matching database containing the same individuals as the target dataset, full knowledge of the data collection mechanism, infinite time and patience (eg Brand et al, 2009). Hundepool et al (2012), in what is effectively a summary of accepted good practice in SDC, make extensive use of worst-case scenarios.

The use of worst-case scenarios makes sense in an academic context: when comparing alternative SDC measures, it provides a convenient common base against which to judge contending ideas. It is not necessarily recommended as a practical model: for example, the SDC programme mu-Argus explicitly uses a worst-case scenario to provide estimates of risk (Brand et al, 2010). Nevertheless, the 'objectivity' of such a scenario (and its apparent popularity as a 'norm') appeals to data controllers. Moreover if government owners of data are risk averse (see Buurman et al, 2012, and references therein), the 'better safe than sorry' ethos encapsulated in worst-case scenario planning accords with this psychological outlook.

3. The popularity of 'policing'

In the light of these factors, the 'policing' approach to data security is appealing. First, it does not require knowledge of use of data; second, it does not require knowledge of the users; third, lines of

[1] We distinguish between statement of principles and actual practice. For example, many OECD governments have formal commitments to 'open data' However, these do not always translate into practice.

blame are clearly established for any inappropriate outcome. And while the apparent theoretical support for worst-case scenario planning is not necessary for the policing approach, it is often found in tandem: if you want to apply fixed rules, then a rule which protects you in the worst case would seem to be a sensible approach.

The economics literature also provides support for the policing model. The relevant issue is the ‘principal-agent’ problem, which considers what happens when a principal (for example, the data controller) wants an agent (such as a researcher) to do something (use data safely) which the principal cannot fully control; see eg Kreps (1990) for more detail.

In general, the principal’s options are;

a. Assume that the agent will only follow the instructions which can be monitored (in this case, follow observable protocols), but will make no effort otherwise unless some reward is forthcoming
b. Assume that the agent will put in the necessary effort to achieve the principal’s aims, even if this is not monitored

In the standard (‘neoclassical’) economics presentation, both parties are assumed to be rational, to make full use of any information available, and to seek to maximise their own interests. In these circumstances, the rational agent has no incentive other than to do the minimum to gain the benefits of co-operating; even then, fewer ‘rewards’, or more difficulty in spotting bad behaviour, can mean the agent always does the minimum possible. The principal, knowing this, will only rationally choose option (a) above.

In terms of data security, this translates into simple instructions for the principal/data controller:

- Inform the researcher of all security measures
- Ensure that the agent/researcher is fully informed of penalties
- Do not inform the researcher of your ability to monitor poor behaviour
- If possible, identify a reward mechanism that rewards good behaviour (ideally, one that can be extended indefinitely to continue to reward good behaviour)

This should lead to the researcher calculating costs and benefits and – hopefully – coming to the right conclusion: that compliance with security practices has a higher expected value than misbehaving. When the objectives of both principal and agents are aligned in this way, a stable outcome results. The principal can try to improve the outcome by either increasing monitoring or by increasing the penalties for misbehaviour; either way, this leads to the policing model where a potentially disruptive influence is ‘incentivised’ to do the right thing.

4. Alternative perspectives

The discussion in the previous section focused on “rational” solutions to data access: the use of models and objective measures in a world where individuals act logically in acquiring and using factual data.

However, there are several objections to this perspective, empirical and theoretical.

4.1 Rationality

Although a fundamental tenet of much economic thinking, there is very little evidence to suggest that humans react in the 'rational' way that modellers predict. In Kahnemann (2012), the Nobel Prize-winner brings together his life work, and the work of others, to demonstrate that rational decision-making is the exception rather than the rule. Decisions are at least as likely to be influenced by memories, prejudices, and chance events in the environment as they are by cold logic. Moreover, humans exhibit strong state dependency: change in circumstances quickly become the new norm, meaning that all actions which result in a change of state in the world change the way all future decisions are taken.

Mainstream economists would argue that this is simply a case of 'bounded rationality': given the infinite amount of data collection needed to make a truly informed choice, humans collect only as much information as they feel they need to make a sensible choice. The problem with this response is that bounded rationality is fundamentally tautological: a decision cannot be irrational, and so if it appears so this is only because the boundaries have not been identified appropriately. A more serious criticism is that experimental studies show that irrational (in the sense of being inconsistent and unexplained) decision making is a genuine and observable phenomenon even when 'boundaries' are accounted for.

4.2 Organisational legitimacy

A developing field in criminology has been the question of 'organisational legitimacy': the idea that lawful or, more widely, 'moral' behaviour is affected by the way the policing is carried out (Hough et al, 2013). If an individual believes that the police act appropriately to enforce fair laws, then that individual is more likely to operate in accordance with the law – not because he or she is more concerned about being found out, but because the law and law enforcement seems 'fair'. This should then translate into cost-effective policy outcomes, as the public then becomes self-policing.

This idea, and the implied outcomes of both better and cheaper policing, has provoked much interest in the US, and more recently in the UK (Hough, 2012); Drew et al (2012) note that the UK Ministry of Justice has actively promoted the idea, and the Metropolitan Police (the London force) now requires training in maintaining legitimacy for all senior officers. Jackson et al (2011, 2012) summarise a broad range of evidence from the US and Europe, drawing on both the criminological and psychological literature as well as dedicated survey evidence, and conclude that the benefits from a positive 'willingness to be policed' are real and achievable.

This approach suggests that a sense of 'fairness' is important in encouraging compliance with laws and procedures. The difficulty is that such a concept is hard to pin down, based upon both relative and absolute perceptions of how oneself and others are and could be treated.

4.3 Social and group effects

The rationalising individual model does not recognise group influences such as peer pressure. However, experimental studies have repeatedly shown that humans are strongly influenced by group members. For example, it has been demonstrated that, if all members of a group bar one answer "x" to a question, the last person to respond is much more likely to answer "x" as well, even though he or she might know that the answer is "y". Other experiments have shown individuals willing to lie or deny their own testimony to go along with a group; for an extensive discussion of these and similar results, see Kahneman (2012)

The Grameen Bank model of microfinance in Bangladesh provides a useful analogy in the application of peer pressure to ensure compliance (UN, 1998). Where access to finance is limited and therefore a precious resource, each member of a farming community contributes to a fund. In times of difficulties, each member may borrow from the fund, on the condition that they make higher contributions when resources are more plentiful. Belonging to a community increases the cost to any individual member considering reneging on the promise to replenish the fund. The direct consequence of the refusal to contribute, or defaulting on a debt, reduces future access to funds; but UN (1998) and Banerjee and Duflo (2011) argue that it is peer pressure, and the potential for ostracism from the community, that drives the very low default/withdrawal rates.

Likewise, anecdotal evidence from the UK Data Service Secure Lab suggests that the 'community self-enforcing' effect is important for ensuring safe use of data facilities. Access to the Secure Lab is provided to researchers largely on the basis of trust, and so the foolish action of one member abusing that trust (for example, identifying and exposing an individual entity from a dataset) may result in the loss of service for everybody. This communal disaster is highlighted at compulsory training courses which researchers wishing to access the facility must attend: researchers are reminded that their actions could lead to the loss of service for many hundreds of others, and the bad behaviour of others affects their ability to use data. The experience of the Secure Lab has been that this emphasis on collective responsibility generates a community of researchers ensuring that each researcher abides by the conditions of access properly. This is particularly true where large concentrations of research colleagues access the same facility (such as the forty-odd researchers from the Centre for Economic Performance using the Secure Lab).

The organisational aspect is one of the 'community parameters'. A second concerns the subject discipline. This is particularly relevant to quantitative social sciences where small clusters of researchers work in the same field, and access the same sources of microdata. In this example, a researcher who commits a grievous crime leading to the closure of a facility such as the Secure Lab, will adversely affect other researchers in the same discipline. The researchers may not necessarily work at the same institution, but at relatively small conferences (applied labour economics for example) where researchers know each other well, it will become obvious which researcher committed the offence that led to everybody's access to the same microdata being denied.

Therefore with respect to access to confidential microdata via a secure facility, the community parameters are defined by these organisational and discipline elements. Community cohesion will be stronger still where a group of researchers working in the same discipline also reside at the same organisation. Instilling these values, and creating a 'community' of researchers, has formed the central plank of the Secure Lab's security model. Directly monitoring some 600 researchers with a small number of staff would be impossible, but fostering the principles of working as a community, leading to self-enforcement by community members themselves, is a cost-effective and efficient strategy.

5. Positive accounting for the human factor

The above sections illustrate that decision-making is not a rational activity carried out in a vacuum. On the contrary, decision-making is a much more random event; however it is influenced in predictable ways by social and group interactions, and there is evidence to suggest ways that perceptions of ‘doing the right thing’ can be directed.

The traditional ‘policing’ view of research data access described above is still a common conceptual approach to data release. Where there is little understanding of researchers and their objectives, the bluntness of the policing is irrelevant to the goals of an organisation primarily focused on risk avoidance and which sees all access as problematic. As already noted, academic research focuses on the ‘data intruder’ as a risk that data providers must be aware of when providing access to data. Combating the ‘data intruder’ involves heavy policing and restricted access.

This assumes that the objectives of researchers and data owners are different. However, there is no reason for this to be the case; in fact, Welpton and Ritchie (2012) and Desai and Ritchie (2009) argue that researchers can demonstrably and reliably become self-policing.

Researchers are as conscious of the need for data protection as much as data owners. Academic researchers in particular, play a ‘repeated game’ throughout the course of their careers. Researcher outcome one will be followed by research outcome two, and three and four etc. going into the future. It is therefore in their interest that data are available to them, and therefore interested in ensuring data and access to data are sufficiently protected. Were research a ‘one-shot’ game then their incentives for protecting data would be different[2].

In addition to their interest in the long-term survival of data access, researchers are particularly interested in ensuring the quality of the data they access is maximised (as poor quality data will affect research outcomes, in terms of results and the proportion of time ‘adjusting data’, e.g. cleaning for analysis).

While researchers may share the same objectives as data owners, they do not necessarily share the same values or perceptions of risk of the data owners. For example, the data controller will typically view the researcher as a security risk; very few researchers understand or recognise that categorisation. This is because of the risk is almost always presented to the researcher in terms of the intruder model, which researchers do not see as relevant to themselves. In this the researcher is correct; in fifty years of data access there is no evidence to support the malicious misuse of data by accredited researchers.

There are however regular cases of accidental misuse of data, and deliberate misuse by researchers wanting to make life easier for themselves (but not breach confidentiality). In that sense, the data controllers are correct: researchers do constitute a security risk. Dealing with such a risk implies a completely different strategy which recognises the interest, and perhaps active co-operation, of researchers. Unfortunately, the policing approach to researcher management is more likely to exacerbate conflict.

However, Desai and Ritchie (2009) and Welpton and Ritchie (2012) note that a change of perception on the part of the data controller can align the objectives of researchers and data owners with minimum ‘policing’. The key is to acknowledge the evidence on the three issues raised above:

- Rationality: researchers do not make rational judgements about risk; on the contrary, they predictably tend to follow the path of least resistance to achieve their aims

[2] In game theory, repeated games typically find that co-operative solutions are both feasible and outperform ‘selfish’ strategies.

- Legitimacy: researchers can be self-policing when they see data security as shared responsibility for a valuable outcome
- Group effects: peer pressure (and ostracism) can influence data security by setting 'norms' for behaviour

The two examples in this section consider how these can be exploited to provide by enhanced security and lower cost, by exploiting the human factor positively rather than seeing it as something to be managed away.

5.1 The Virtual Microdata Laboratory and UK Data Service Secure Lab

The Virtual Microdata Laboratory (VML) and the UK Data Service Secure Lab ('Secure Lab'), are two facilities allowing secure remote access to very detailed microdata for statistical research purposes. The VML was set up by the UK Office for National Statistics in 2003; the Secure Lab, using different technology but the same ethos, began operation on 2011.

Both abandoned the traditional policing model of data access granted to statistics. In the case of the VML, this took place over the first year when it became clear in the mandatory security training sessions that this approach was creating antagonism in researchers. Over time the security training evolved into something much more focused on engagement. The Secure Lab adopted this approach on its inception and continued to develop the training.

The training ethos

The starting point was the 'effective researcher management' strategy of Desai and Ritchie (2009), which emphasised data security as a collaborative venture. Much of the training was devoted to helping researchers understand and empathise with the decision made about the way the facilities were run – creating legitimacy.

The training also emphasised the role of mistake and selfish (but not malicious) actions in creating risk. Rather than warning the researchers not to break the rules, the training explicitly emphasised that mistakes were likely to happen and the key concern was to make sure they were not repeated; owning up to mistakes was rewarded, rather than punished. By reiterating that the function of the lab managers was to help researchers avoid breaking the law, legitimacy of process was established.

Finally, the training worked to develop group responsibility by discussing the risk that misbehaviour by one party could make life worse for all; therefore, there was a need for everyone to be vigilant for abuse of procedures, even if data confidentiality was not breached. Rather than hiding information about monitoring, the VML and Secure Lab training emphasised the fact that continual monitoring was impossible without making the facility unusable; hence researchers had a duty to self-police. While in theory telling people how they can get away with abuse is a terrible idea, in this case it had the desired effect: researchers became self-policing, willing to admit to mistakes and even occasionally 'shop' each other about minor infringements.

In short, the training was explicitly designed to encourage empathy, peer pressure and legitimacy.

System design

If taking the policing approach, the assumption must be that everything must be done to stop researchers doing the wrong thing. This is likely to lead to a very restrictive operating environment. However, as Desai and Ritchie (2009) point out, deliberate misuse of facilities almost always occurs because researchers become frustrated with working practices which they do not understand, and seek to circumvent them.

Hence, if one starts from the assumption that researchers are generally trustworthy, then it is possible to design a system that is less controlling. Researchers then have less incentive to find ways to circumvent the system, and so there is less need for policing and control – a virtuous circle. In short, one is exploiting the researcher's preference for doing the easy thing to ensure that they do the right thing.

This translates directly into operating costs: the VML and Secure Lab operated at between one-third and one-tenth the cost of comparable facilities in the OECD, yet still outperformed on operational measures (source: personal discussions with facilities managers). However, the requirement for face-to face training does increase the fixed costs of access to both researcher and the data controllers.

The net result is that it is possible to design a system based on assumption that researchers do the right thing, which encourages then that behaviour.

Creating Virtual Circles of Trust: Evolution of Behaviour

Evolutionary game theory can provide some insight into how self-enforcement of data access criteria by researchers accessing secure data facilities. Begin with a homogeneous group who possess no information about the correct way of accessing secure data. We then introduce an intervention to researchers wishing to access a secure data facility (for example, providing training on how to access the data safely and statistical disclosure control). All researchers receive this training. There will, however, be some members of the group who do not ingest the training education as much as the others. Therefore we have 'weakly' and 'strongly' trained researchers.

We now combine the 'community self-enforcement' idea from before. In circumstances whereby 'weakly' and 'strongly' trained researchers exist and access confidential data in a secure facility, and a situation of 'community self-enforcement' presides, the diffusion of preferences for data security (given the incentives described above) will occur from the 'strongly' trained to the 'weakly' trained, thereby satisfying the wishes of data owners who wish to ensure that access to their data is safe, because eventually the vast majority of researchers will have 'strong' preferences for safe use.

This introduces dynamism: the human element in data security is an evolving concept, rather than static. Indeed, if we believe that we learn from our mistakes, we therefore adopt stronger preferences for data security, and will encourage others to do so and learn from our mistakes also.

The evolution of data security therefore creates a virtuous circle, sparked by positive enforcement from services such as the VML and Secure Lab. Good behaviour mutates and spreads amongst all the researchers, and everybody with the right incentives, within a community setting, will continually update themselves by learning from past mistakes. Again, there is little requirement for heavy-handed policing of researchers by many staff: the small flutter of a butterfly's wings can cause a tidal wave.

This evolution of researcher behaviour is not only advantageous for ensuring safe use of confidential data, but assists in the development of other areas of data access. For example, development of statistical disclosure control (ensuring results generated from confidential data cannot be used to identify data subjects) is also a key security measure. Researchers generate the results (rather than the data owners or service providers), so their input in developing statistical disclosure control methods is essential.

Within the context of a virtuous circle, researchers will feedback to data owners and service providers about the creation of new types of results that have not been assessed for disclosure in the past. Everybody can work together to formulate a solution for disclosure control of these results, since everybody within the virtuous circle has the incentives to achieve the same goal: safe data access. Everybody then learns from each other in terms of generating 'safe results' in the future.

5.2 The Community Innovation Survey Scientific Use Files [does this add anything?]

The Community Innovation Survey is a three-yearly survey of the innovation activities of businesses in the European Economic Area. Eurostat undertakes to provide the microdata on CD as a 'scientific use file (SUF) for accredited researchers.

Prior to 2013 the approach to creating the SUFs was to follow the standard 'intruder' scenario. As a result, more disclosive variables were hidden or limited, and microaggregation (a form of SDC that perturbs the value of variables) was applied to all the continuous variables in all records in the dataset.

In 2013 Eurostat commissioned a review of the method (summarised in Hafner et al, 2014). The review highlighted that, while the theoretical risk of re-identification was high, the practical risk was significantly lower. In addition, the information had very little commercial value. Allied to the known lack of malicious misuse, the review argued that the data was being perturbed to no practical effect. Anecdotal evidence from Eurostat suggested that the SUF's main use was for teaching.

The review suggested an incentive structure for researchers which reflected those concerns. It also analysed how researchers used this data when they had access to the full dataset. The resulting anonymisation technique microaggregated only one continuous variable, and did so for less than 1% of the records. In theory this makes the data set more sensitive than before, but Hafner et al (2014) argued that the reverse is the case: the practical risk of deliberate misuse remains at a negligibly low level, but the increased research value of the dataset means that researchers may be persuaded to take the security of the data more seriously.

6. Conclusion

Taking a policing approach to data security is appealing but has its flaws. This paper has suggested that a more co-operative approach may be more effective in certain circumstances.

Researchers and data owners do share the same set of overall incentives to ensure that data is made available for use, securely and fairly. Data owners may collect and use data for different purposes to researchers, but the principles of long-term data access, and data access, are of interest to both parties. Rather than viewing researchers with suspicion and enforcing heavy-handed policing techniques, there is scope for data owners and researchers work together to find solutions which bind their incentives and objectives together. This is particularly true when data owners and researchers are informed about each others' objectives and thus understand incentives for accessing data. The approaches mentioned above can work effectively in this environment of shared understanding of objectives and incentives.

This paper has focused on research access to confidential data where the policing approach to data security is demonstrably less effective than an evidence-based approach reflecting human psychology. Nevertheless, there are potentially lessons for the wider data community. The change in perspective to a user-centred model is driven by the recognition of three factors

- co-operation tends to outperform self-interested behaviour
- behaviour and social psychology shows that positive behaviours can be self-reinforcing
- evidence does not support worst-case scenarios

Because much of this discussion is carried out in the public sphere, the perspectives of different groups and the evidence base have been widely discussed. Not all of this is relevant to different organisations. For example, a retail firm's loyalty card data is likely to have significant commercial value; a defence ministry may be subject to cyber-attack irrespective of personnel training.

However, the key point of this paper is that an evidence-based approach to managing the human factor may suggest substantially different ways of approaching the problem. The human factor is widely recognised as one of the knottiest problems in managing data confidentiality; yet the experience of researcher data access suggests the rewards may be significant.

References

Banerjee A. and Duflo E (2011) *Poor Economics: Barefoot Hedge-fund Managers, DIY Doctors and the Surprising Truth about Life on less than $1 a Day.* Penguin.

Bhatta G. (2003) "Don't just do something, stand there! Revisiting the issue of risks in innovation in the public sector". *The Innovation Journal*.

Brand R, Capobianchi A, Domingo-Ferrer J, Franconi F, Giessing S, Hundepool A, Polettini S, Ramaswamy R, van de Wetering A, Torra V, de Wolf P-P (2009) *mu-Argus User Manual*.

Buurman M., Delfgaauw J., Dur R. and van den Bossche S. (2012) *Public sector employees: Risk averse and altruistic?*, CESifo Working Paper: Behavioural Economics, No. 3851

Desai T. (2012) "Maximising Returns to Government Investment in Data", presentation to IASSIST 2012, Vancouver.

Desai T. and Ritchie F. (2010) "Effective researcher management", in *Work session on statistical data confidentiality 2009*; Eurostat.

Desai T. Ritchie F. and Welpton R. (2014) "The Five Safes", working paper, University of the West of England

Drew H., King A. and Ritchie F. (2013) *Impact Evaluation: Workplace Employment Relations Survey and European Social Survey*. Final report. Economic and Social Research Council. February

Hafner H-P., Lenz R. and Ritchie F. (2014) *User-focused threat identification for anonymised microdata*. Presentation to Conference of European Statistics Stakeholders, November.

Hough, M. (2012) 'Researching trust in the police and trust in justice: A UK perspective', *Policing and Society, 22*, 3, 332-345.

Hough, M., Jackson, J. and Bradford, B. (2013 in press) 'Trust in justice and the legitimacy of legal authorities: topline findings from a European comparative study' in Body-Gendrot, S., Hough, M., Levy, R. Kerezsi, K. and Snacken, S. (2013, in press) *European Handbook of Criminology* (edited volume). London: Routledge.

Hundepool A., Domingo-Ferrer J., Franconi L., Giessing S., Schulte Nordholt E., Spicer K., de Wolf P-P. (2012) *Statistical Disclosure Control*. Wiley .

Jackson, J., Hough, M., Bradford, B., Pooler, T., Hohl, K. and Kuha, J. (2011) *Trust in Justice: topline results from Round 5 of the European Social Survey. ESS Topline Results Series Issue 1***.** London: City University.

Jackson, J., Hough, M., Bradford, B., Hohl, K. and Kuha, J. (2012) *Policing by consent: UK evidence on legitimate power and influence. ESS Country Specific Topline Results Series Issue 1.* London: City University.

Kahneman D. (2012) *Thinking, fast and slow*. London: Penguin Books.

Kreps D.M. (1990) *Microeconomic Theory*. Prentice-Hall

Lofstedt R.E. (2004) “The swing of the regulatory pendulum i Europe: from precautionary principle to (regulatory) impact analysis”. J. Risk and Uncertainty v28:3 pp237-260

Moore M.H. (2010) "Break-Through Innovations and Continuous Improvement: Two Different Models of Innovative Processes in the Public Sector". Public Money & Management January 2005 v44

OACG (1998) *Innovation in the Federal Government: the Risk Not Taken*. Public Policy Forum Discussion Paper, Office of the Auditor-General of Canada.

Ritchie F. (2014a) “Resistance to change in government: risk, inertia, and incentives”, paper presented to Organisation Studies workshop, May

Ritchie F. And Welpton R. (2012) "Sharing risks, sharing benefits: Data as a public good", in *Work session on statistical data confidentiality 2011*; Eurostat.

UN(1998) *The role of microcredit in the eradication of poverty.* United Nations. Report of the Secretary-General

Welpton R. and Ritchie F. (2012) "Incentive compatibility in data security", presentation to IASSIST 2012, Vancouver

Recent UWE Economics Papers

See http://www1.uwe.ac.uk/bl/research/bristoleconomics/research for a full list

2014

1413 **Addressing the human factor in data access: incentive compatibility, legitimacy and cost-effectiveness in public data resources**
Felix Ritchie and Richard Welpton

1412 **Resistance to change in government: risk, inertia and incentives**
Felix Ritchie

1411 **Emigration, remittances and corruption experience of those staying behind**
Artjoms Ivlevs and Roswitha M. King

1410 **Operationalising 'safe statistics': the case of linear regression**
Felix Ritchie

1409 **Is temporary employment a cause or consequence of poor mental health?**
Chris Dawson, Michail Veliziotis, Gail Pacheco and Don J Webber

1408 **Regional productivity in a multi-speed Europe**
Don J. Webber, Min Hua Jen and Eoin O'Leary

1407 **Assimilation of the migrant work ethic**
Chris Dawson, Michail Veliziotis, Benjamin Hopkins

1406 **Empirical evidence on the use of the FLQ formula for regionalizing national input-output tables: the case of the Province of Córdoba, Argentina**
Anthony T. Flegg, Leonardo J. Mastronardi and Carlos A. Romero

1405 **Can the one minute paper breathe life back into the economics lecture?**
Damian Whittard

1404 **The role of social norms in incentivising energy reduction in organisations**
Peter Bradley, Matthew Leach and Shane Fudge

1403 **How do knowledge brokers work? The case of WERS**
Hilary Drew, Felix Ritchie and Anna King

1402 **Happy moves? Assessing the impact of subjective well-being on the emigration decision**
Artjoms Ivlevs

1401 **Communist party membership and bribe paying in transitional economies**
Timothy Hinks and Artjoms Ivlevs

2013

1315 **Global economic crisis and corruption experience: Evidence from transition economies**
Artjoms Ivlevs and Timothy Hinks

1314 **A two-state Markov-switching distinctive conditional variance application for tanker freight returns**
Wessam Abouarghoub, Iris Biefang-Frisancho Mariscal and Peter Howells

1313 **Measuring the level of risk exposure in tanker shipping freight markets**
Wessam Abouarghoub and Iris Biefang-Frisancho Mariscal

1312 **Modelling the sectoral allocation of labour in open economy models**
Laura Povoledo

1311 **The US Fed and the Bank of England: ownership, structure and ‘independence’**
Peter Howells

1310 **Cross-hauling and regional input-output tables: the case of the province of Hubei, China**
Anthony T. Flegg, Yongming Huang and Timo Tohmo

1309 **Temporary employment, job satisfaction and subjective well-being**
Chris Dawson and Michail Veliziotis

1308 **Risk taking and monetary policy before the crisis: the case of Germany**
Iris Biefang-Frisancho Mariscal

1307 **What determines students’ choices of elective modules?**
Mary R Hedges, Gail A Pacheco and Don J Webber

1306 **How should economics curricula be evaluated?**
Andrew Mearman

1305 **Temporary employment and wellbeing: Selection or causal?**
Chris Dawson, Don J Webber and Ben Hopkins

1304 **Trade unions and unpaid overtime in Britain**
Michail Veliziotis

1303 **Why do students study economics?**
Andrew Mearman, Aspasia Papa and Don J. Webber

1302 **Estimating regional input coefficients and multipliers: The use of the FLQ is not a gamble**
Anthony T. Flegg and Timo Tohmo

1301 **Liquidity and credit risks in the UK’s financial crisis: How QE changed the relationship**
Woon Wong, Iris Biefang-Frisancho Mariscal, Wanru Yao and Peter Howells

2012

1221 **The impact of the quality of the work environment on employees’ intention to quit**
Ray Markey, Katherine Ravenswood and Don J. Webber

1220 **The changing influence of culture on job satisfaction across Europe: 1981-2008**
Gail Pacheco, De Wet van der Westhuizen and Don J. Webber

1219 **Understanding student attendance in Business Schools: an exploratory study**
Andrew Mearman, Don J. Webber, Artjoms Ivļevs, Tanzila Rahman & Gail Pacheco

1218 **What is a manufacturing job?**
Felix Ritchie, Andrew D. Thomas and Richard Welpton

1217 **Rethinking economics: Logical gaps – empirical to the real world**
Stuart Birks

1216 **Rethinking economics: Logical gaps – theory to empirical**
Stuart Birks

1215 **Rethinking economics: Economics as a toolkit**
Stuart Birks

1214 **Rethinking economics: Downs with traction**
Stuart Birks