This item was submitted to [Loughborough's Research Repository](#) by the author.
Items in Figshare are protected by copyright, with all rights reserved, unless otherwise indicated.

Data sharing and crime reduction: The long and winding road.

PLEASE CITE THE PUBLISHED VERSION

PUBLISHER

© Perputity Press

LICENCE

CC BY-NC-ND 4.0

REPOSITORY RECORD

Brookes, Stephen, Kate Moss, and Ken Pease. 2019. "Data Sharing and Crime Reduction: The Long and Winding Road." figshare. <https://hdl.handle.net/2134/890>.

Data-sharing and Crime Reduction: The Long and Winding Road

Stephen Brookes, Kate Moss and Ken Pease¹

The Crime and Disorder Act 1998 charges responsible authorities with devising and implementing strategies for community safety. Responsible authorities comprise police and local authorities, working as partnerships. Criteria for the permissible exchange of relevant data are to be found in the Act. In practice, partnerships have experienced difficulties in reaching agreement about data-sharing. This paper looks at the legal background to data-sharing, its limitations, best practice, and the potential consequences of lowering barriers to information exchange.

Key Words: Data-sharing; crime reduction; partnerships

Introduction

The rhetoric of the Crime and Disorder Act 1998 emphasises partnership. This is reflected in the Act's specification of the local structure charged with responsibility for crime reduction. Yet when crime reduction organisers gather, and talk turns to data protection issues, four facts swiftly become evident:

- police data protection officers vary massively in the presumptions they bring to their work;
- some officers interpret data protection so restrictively that the community safety enterprise is compromised;
- senior police officers do not take an active role in shaping agreements on data sharing; and
- crime reduction and community safety organisers are often unclear about the action implications of shared data, which feeds the presumption *against* data exchange.

A common understanding of appropriate data-sharing is important for three reasons:

- The best predictor of crime is prior crime against the same target (see for example Pease, 1998). Reducing crime depends in part on prompt action after crime victimisation, by both police and partner agencies. How such action is organised depends crucially on disaggregated victimisation data.
- Differences in data-sharing practices across Crime and Disorder Reduction Partnerships (CDRPs) limits the spread of good practice based on local data-sharing agreements. This is often given voice (either realistically or as an excuse) as 'we can't do that here because we can't get the data'.

- Senior police officers will remain reluctant to interfere with the way in which data protection officers do their work until it can be shown to be capricious by reference to agreed national standards.

As crime reducers, we would find it convenient if a common understanding regarding data-sharing could be reached which allowed controlled access to data, and which would correspondingly provide information on crime reductive efforts to *all* those in a position to advance the cause of crime reduction by means which are supported by evidence, or by plausible extensions of such means. The whole emphasis of crime reduction thinking, from the Morgan Report (1990) onwards, has been to recognise that agencies other than the police routinely make decisions with crime consequences, and, by involving these agencies in crime reduction, to co-locate responsibility for community safety. Such a radical re-positioning of crime reduction responsibilities requires a trade-off between crime reduction and the maintenance of privacy. We believe that the currently crucial goal is agreement. Not necessarily the kind of agreement that we ourselves would favour, but an agreement which we might find sub-optimal would nonetheless afford a level playing field for community safety partnerships, and allow tactics which maximised the amount of relevant help afforded to citizens by routes consistent with data-sharing arrangements. In short, as in so many areas of life, the perfect may be the enemy of the good, if perfection takes a long time to achieve. A somewhat radical alternative is proposed in a companion article, which is based on a schedule of contingent actions whereby the agreement is *not* to share data routinely, but to act in agreed ways in circumstances designated by partner agencies. This has advantages over blanket agreements to share data, which is an approach which could be criticised. However, the present article develops the more standard, and probably realistic, approach to data-sharing.

The legal background

There are currently no legislative controls on the exchange of non-personal data. The exchange of personal data is covered by legislation. Certain aspects of both administrative and common law are also relevant, and these will briefly be highlighted. One of the main thrusts of the Crime and Disorder Act 1998 (hereinafter referred to as 'CDA') was partnership working. In line with this, s.115 of CDA allows the disclosure of personal information to the police, local authorities, probation committees and health authorities for any legitimate activity associated with the reduction of crime. It states that:

Any person who, apart from this subsection, would not have the power to disclose information –

- a. to a relevant authority; or
- b. to a person acting on behalf of such an authority,

shall have the power to do so in any case where the disclosure is necessary or expedient for the purposes of any provision of this Act.

In essence s.115 provides a statutory gateway for information flow. It gives partnerships the legal power to exchange.

Section 17 of the same Act statutorily obliges all local authorities to consider crime and disorder in their decision-making processes. To do this, prompt case-by-case exchange of personal information about actual and potential crime victims between local authorities and the police—

in both directions—seems essential. The local authority needs to know which streets, homes and businesses are priority claimants on improved security provision, and for this they need information from crime reports. The police need to know which homes and individuals fall into high-risk categories. To take an example, Ellingworth and Pease (1998) showed that those about to move home, and those who have recently moved, have temporarily elevated levels of risk of burglary. To be serious about the lowering of such risks, the police need to know which households are in the throes of moving. In other words, to adhere to s.17 of the Act, working arrangements under s.115 must be in place.

Whilst CDA seems to provide legal authority for the disclosure of information, uncertainty enters when we consider countervailing rights. Heed must be taken of other statutory or common law restraints on disclosure, including human rights and the law of confidence. It is also necessary to be mindful of the fact that according to the principles of administrative law, any authority exercising such a statutory power must do so for the purpose that the statute specifies.

The Data Protection Act 1998 exists to ensure that personal data are treated and used properly. As such, it should not prevent data-sharing *per se* but should be seen as requiring clear protocols for data exchange. It is important that partnerships also set up their own protocols for data exchange, to ensure clarity regarding the use and exchange of data between partners and the responsibilities and liabilities that go along with this, possibly against some generic standards; otherwise everyone will be reinventing wheels of varying degrees of circularity. The Act sets out eight basic principles of data protection, which are aimed at ensuring acceptable exchange principles. According to Schedule 1 of the Act, data must:

- be fairly and lawfully processed;
- not be further processed in a manner incompatible with the purpose for which they were obtained;
- be relevant, adequate and not excessive;
- be accurate;
- not be kept longer than necessary;
- be processed in accordance with the data subject's rights;
- be secure; and
- not be transferred to countries without adequate protection.

The common law tort of breach of confidence is also relevant. Many aspects of English common law have developed to protect an individual's rights to privacy, and can provide for damages in the event of a breach of statutory duty. This could occur where the recipients of information exchanged under data-sharing principles either take unfair advantage of this information, or where it is later used in an unauthorised way. It is thus possible for the law of breach of confidence to protect against the unauthorised use or disclosure of some types of confidential information. Partners who exchange data need to be aware of their obligations and the extent of this sort of duty. A recent case which dealt with these issues is *Hellewell v Chief Constable of Derbyshire* [1995] 1 WLR 804. This case concerned the legitimate use of a 'mug shot'. The

plaintiff had 32 previous convictions, 19 for offences of dishonesty. His photograph had been circulated to shopkeepers who were experiencing thefts as depicting an individual likely to cause problems. The plaintiff had become aware of this and alleged breach of confidence on the part of the police. It was held that the police had acted in good faith, and that the dissemination of the photograph had been limited to shopkeepers in the shop watch scheme. It was, the court held, beyond doubt that the use made by the police of the photograph was lawful. During the course of the judgement, Dillon LJ commented that;

...there manifestly must be some limitation on the purposes for which seized documents can be used. Search and seizure under statutory powers constitute fundamental infringements of an individual's immunity from interference by the State with his property, privacy...[and] fundamental human rights... In my judgement, subject to any express statutory provision in other Acts, the police are authorised to seize, retain and use documents only for public purposes related to the investigation and prosecution of crime and the return of stolen property to the true owner.

The role of the Data Protection Commissioner is also important, for two reasons. First, the Commissioner's role is to promote good practice and enforce compliance with the Data Protection Principles by assessing complaints and bringing prosecutions for breaches of the criminal provisions of the Act. Second, it is possible for partnerships to keep abreast of legal developments relating to the misuse of data by maintaining regular contact with the Commissioner.

With the current absence of case law specific to this area, one question remains unanswered within the legal framework of data-sharing: whether a data-sharing partnership constitutes a legal entity. This is an important point, since there is an increasing tendency to refer to CDRPs as 'virtual organisations'. For example, if a case arose where an aggrieved citizen wished to sue for the misuse of personal data, the question remains: whom exactly would he/she sue?

Limitations to data-sharing

There are inevitably a number of limitations to data-sharing. These are not insurmountable, but cross the boundaries of cultural, political and practical limitations (including any propensity for sheer organisational inertia). Common issues that should be addressed are:

- the identification of core data;
- how often data should be trawled;
- who should be responsible;
- who should pay;
- what the quality of the data will be like; and
- whether we should set up any protocols.

To drive strategic needs, data should be trawled and analysed at least once every quarter. This may not be often enough to drive operational needs. Physically extracting data can be difficult when partners use different systems. The police already have a culture of some data analysis, and in most cases feel ahead of the game in this respect. However, even police data analysts are not trained to retrieve or deal with data other than their own. To undertake this requires

either in-house training or the appointment of a partnership analyst—which is costly. Other issues which then become relevant are: to whom does the analyst ‘belong’, and where should his/her office be located? This might appear trivial, but these questions require answers to avoid inter-departmental or agency turf wars. The potential quality of the data can also be important in hindering the effective sharing of data. Data exchange means losing control of that data. This can be potentially frightening or embarrassing for the owner if the data appears to be ambiguous, dirty or unflattering. Cleaning data adds an extra cost dimension to this process. The Government Office for the East Midlands (GO-EM) has funded five analysts in Derby and in Nottinghamshire. These posts have been red-circled (they only carry out partnership work). A similar approach has been adopted in London, of which less detail is known given the authors’ experience in the East Midlands. The initial funding for these posts was through the Partnership Development Fund. There are still cultural, practical and physical difficulties to doing this work, but GO-EM is committed to pushing forward with the ideology of data exchange. For these reasons it is important to set up generic protocols for data exchange which all partners feel happy to sign up to and which can facilitate useful exchange, whilst at the same time ensuring both for data owners and the public that the data are not misused.

Best practice

Perhaps the best example of successful data exchange is that demonstrated by Project Jupiter. This project is currently being piloted by GO-EM and the Government Office for the South West, and seeks to collect data at local level from multiple agencies such as the police, councils, health, ambulance, fire and probation services.

Jupiter establishes that for any partnership to achieve successful data exchange the partners must believe in data-sharing in the first place. Early on, GO-EM saw the benefits which could come from encouraging data exchange amongst the representatives within the CDRPs, and worked hard to fund appropriate technology to facilitate this. This involved the appointment of a project manager who oversaw the implementation of the project by disseminating information about data exchange practices and procedures to all CDRPs within the region. This was backed up with substantial funding, which enabled CDRPs to purchase the relevant hardware and software consistent with developing data exchange procedures, and which also provided for the appointment of analysts to undertake this work.

Of the 40 CDRPs in the region, approximately 75 per cent now have access to Jupiter data exchange. This project is still in the early stages of a long-term enterprise. Some CDRPs have progressed faster with the implementation of specific data exchange procedures than have others. Whilst some are mapping hot spots and geo-coding various types of core data, others are still negotiating with their partners for core data sets, and have only recently appointed analysts. Others are only talking at the very basic level about whether to sign a protocol.

At this stage, it became clear to GO-EM that there was a certain amount of what we might call anecdotal or experiential evidence about the problems encountered with implementation. Whilst the model itself was not thought to be in question, GO-EM felt that it was timely to commission research to evaluate the current status of Jupiter in terms of levels of penetration and of the presenting relationships between need and provision, in order to inform a strategic direction for Jupiter data-sharing in the future, and to establish how this could be used to drive crime reduction initiatives.

First impressions established that successful data-sharing partnerships need to take a number of steps to overcome the barriers to data-sharing, which are:

- to establish a partnership of key agencies and to secure funding to finance it;
- to agree objectives based on the most recent crime audit;
- to sign a regularly revised data-sharing protocol with partners;
- to set up an analysis capability;
- to install the appropriate technology to enable data exchange;
- to initiate data-sharing and analysis and to share outcomes with all partners;
- to monitor, evaluate and give feedback to improve performance; and
- to establish support and leadership at the highest level within each CDRP.

The culmination of the study in March 2003 established that the common problematic themes which emerged from the research were related to issues of focus, communication and leadership. In terms of focus, most CDRPs over-emphasised the need for populating systems with data without focusing in on what could be achieved with that data or how it could be used to solve problems. As a result of this finding, GO-EM is currently in the process of setting up a pilot project in which data-sharing and analysis will be used specifically to reduce domestic burglary within two residential areas of Nottinghamshire. It is worth noting that Nottingham has the second-highest level of domestic burglary in England and Wales, and to date substantial funding has been allocated to this problem; however, levels of domestic burglary are still not reducing. In terms of communication, the research highlighted that there is a need for awareness-raising in relation both to data protection and the benefits of data-sharing which could be disseminated better through illustrations of best practice within the region. Finally, lack of support at the highest level was also evident, making it clear that both Chief Executives and Divisional Police Commanders needed to engage with and support the concept of data-sharing at partnership level. One way of taking this forward (having had pump-priming funds from GO-EM at the outset) would be for them to allocate their own resources to data-sharing projects, both to mainstream analysis and to fund permanent posts for analysts.

It is vital that issues such as these do not become sidelined, not least because of the links that this work has with statutory obligations such as that encapsulated in s.17 CDA. Movement by CDRPs to mainstream this sort of crime reductive work would underpin this obligation and provide tangible evidence that they are taking these obligations seriously.

There will doubtless be many more issues in relation to the real barriers of data-sharing, and some interesting recommendations that could be made. However, this research is also important for other reasons. It signals that GO-EM is committed to playing its part in leading the continuing strategic direction of this project, which may pave the way for other regions and other CDRPs to move forward in the same fashion. It also emphasises the benefits of collaborative work amongst all CDRP partners in the wider picture of crime reduction.

Which data: exchanged with whom?

It is clear from s.115 of CDA that the government's view is that data exchange, properly done, can help to reduce crime and disorder whilst at the same time helping to remove barriers which might previously have hindered partnerships. However, one question remains: is the government

looking for a quick fix with data exchange? The government has funded data exchange initiatives, but there will be no quick fix—it will take time to see real results from data-sharing. This needs to be made clear at the highest level if any common understanding regarding data-sharing to reduce crime is to be reached.

In the meantime, where you can go with this is unknown as yet. The problem is you cannot ‘suck it and see’ because data-sharing takes time, commitment, effort and money. There is still a need to be innovative and pursue analysis to see where it goes. As a result, it is essential that protocols are drawn up which are flexible enough to allow for innovation. CDRC analysts need to be prepared to look at different things and use data in innovative ways. One example of this was recently given by Sherman (2001), where in the case of a serial rapist the police used tactical crime-mapping and analysis, previously used only to map the movement of animals, to build up a picture of the offender’s movements.

An acceptance that the outcomes of data-sharing will be different for different agencies is important and will help to dispel the ‘what’s in it for me’ barrier. Common sense dictates for example that the police have different priorities to social services, and that any analysis should take account of this fact. This will also impact on the type of analysis that can be done. Partners should be careful that they do not exclude each other from that analysis. In this sense we could ask the question: ‘How effective is multi-agency analysis?’

Having said all this, data-sharing with partnerships is of key importance, for a number of reasons:

- it can help identify what a CDRC’s particular problems are;
- it can be used to concentrate on the issues that are really problematic;
- it allows for the possibility of integrating different methods of analysis, such as mapping, with other data, particularly victimisation data—because if you want to know where crimes will occur, you only have to look at where they happened before—it’s likely to be the same place;
- it allows us to focus on issues like what action data-sharing actually implies, eg if all burglars get in through inadequate back doors, we need to make back doors less inadequate, no matter who lives there—a single parent, a family or an old age pensioner; and
- it brings us to the really crucial question with data-sharing, and that is the following.

Who needs to know what and why?

We need to establish the answer to this categorically if we are to move forward with data-sharing. At the moment if there is one thing lacking it is focus. By this we mean there has got to be an answer to the question: ‘Why do people want to share data?’ For example, if you wanted to share data to show that deprivation was associated with victimisation, you would need also to be able to explain why you wanted to show it. The reason this is worth mentioning is that experience seems to show that people want to share data mostly on the basis of some simple associations between things like poverty, deprivation and crime. It is not yet apparent that people have nicely focused views about what they would potentially do with the presenting relationships between crime and other data. Consequently, it would be a bonus to see them nailed to the wall about why they want other people’s data because only then will the true benefits of data exchange be fully realised.

Notes

- 1 Stephen Brookes is Crime Reduction Director, Government Office for the East Midlands. Kate Moss is Programme Director for the MSc in Criminology and Criminal Justice, Department of Social Sciences, Loughborough University (currently seconded to Project Jupiter at the Government Office for the East Midlands); email: K.R.Moss@lboro.ac.uk. Ken Pease is Professor of Criminology, University of Huddersfield, and Visiting Professor, Jill Dando Institute of Crime Science, University College London.

References

- Ellingworth, D. and Pease, K. (1998) Movers and Breakers. *International Journal of Risk, Security and Crime Prevention*. Vol. 3, No. 1, pp 35–42.
- Home Office (1990) Safer Communities: The Local Delivery of Crime Prevention Through the Partnership Approach (the Morgan Report). London: Home Office.
- Pease, K. (1998) *Repeat Victimisation: Taking Stock*. Crime Detection and Prevention Paper No. 90. London: Home Office.
- Sherman, T. (2001) *The Role of Tactical Crime Analysis in Serial Rape Investigation*. Paper presented at the First Advanced Crime Symposium, Denver, CO, June.