Research Ethics Review (2010) Vol 6, No 1, 3–9
Received 13 October 2009, accepted 17 November 2009

Original paper

The problem of proliferation: guidelines for improving the security of qualitative data in a digital age

JUDITH ALDRIDGE, JUANJO MEDINA and ROBERT RALPHS
School of Law, University of Manchester, UK.

Email: judith.aldridge@manchester.ac.uk

High profile breaches of data security in government and other organizations are becoming an increasing concern amongst members of the public. Academic researchers have rarely discussed data security issues as they affect research, and this is especially the case for qualitative social researchers, who are sometimes disinclined to technical solutions. This paper describes 14 guidelines developed to help qualitative researchers improve the security of their digitally-created and stored data. We developed these procedures after the theft of a laptop computer containing highly sensitive data from the home of a fieldworker. This paper introduces the 'principle of proliferation': digitally-created and stored files (like voice recordings of interviews and text files of their transcriptions) tend to proliferate during the course of a research project by virtue of fact that they can and are copied and shared as research progresses from data collection through to analysis and archive. Our guidelines were designed as concrete strategies that researchers embarking on a project can employ, particularly researchers working in teams, to accommodate this proliferation and reduce it where possible.

Keywords: *digital data, data proliferation, guidelines, security, qualitative*

Introduction

In this paper we describe some strategies developed to improve the security of our digitally-created and held qualitative data (involving interviews with gang members) after the theft of a laptop computer containing highly sensitive data from the home of a fieldworker. Over the past few years, high profile breaches of security in the UK and internationally have made headline news, including, for example, the loss of 25 million Child Benefit records by HM Revenue and Customs [1,2]. It seems that the capacity for more and more data to be stored on smaller and more portable devices in itself makes maintaining security a tricky affair. Data security is becoming an increasing concern amongst members of the public. In a survey conducted by the Information Commissioner's Office, 94% of people listed 'protecting personal information' as their top concern, a ranking equal with concerns about crime [3]. This wariness is likely to impact on the willingness of members of the public who are our potential participants to agree to participate in academic research.

Academic researchers do not as a rule talk about the loss of their research data in the books and journal articles they write describing their research. Perhaps academic researchers have yet to be the victims of this kind of loss; or perhaps they are reluctant to come clean about breaches of their data security protocols. Whatever the case, reports about the loss of research data by academic researchers have yet to make news headlines in the same way that happens for government and other public organizations – but it must only be a matter of time.

After the loss of data we experienced, we thoroughly reviewed our data security procedures and found them to be lacking. In presenting here our revised procedures for improving the security of digitally-held data for qualitative researchers, we reflect on our experience of carrying out the ethnographic research 'Youth Gangs in an English City'[1] [4-10]. The guidelines we present in this paper take into account what we refer to as the 'principle of proliferation': versions and copies of qualitative data held digitally proliferate quickly as a result of being held: on different storage devices (voice recorders, laptops, desktops, memory sticks), in different versions (voice, text), in various physical locations (office, home, in the field), by individuals with particular roles on a research team (managers, fieldworkers, interviewers, transcribers), and during different phases of the

[1] ESRC funded research 'Youth Gangs in an English City' REFERENCE No. RES-000-23-0615

research (data collection, data analysis, data archive). The 'lifetime' of one interview, for example, would regularly give rise to dozens of versions and copies in a fairly small research team like ours was.

Professional academic associations usually require researchers to take reasonable steps to ensure that data are preserved in a confidential and secure manner, for example by taking 'extreme care in delivering or transferring any confidential data, information, or communication over public computer networks [and remaining] attentive to the problems of maintaining confidentiality and control over sensitive material and data when use of technological innovations, such as public computer networks, may open their professional and scientific communication to unauthorised persons.' [11]. However, guidance of this sort is usually short on the specifics of how to achieve these aims. Moreover, where advice to qualitative researchers is concerned, the reality that many of us create and store our data digitally is often not adequately recognised, as evidenced in this question-and-answer guidance provided in the context of formal guidance for researchers set out by the British Society of Criminology [12]:

> Q: I've got piles of interview data for my PhD but nowhere to keep the material. I share an office with five others and have two drawers in a filing cabinet but the key has been lost. What am I meant to do with all the data, and does my department have an obligation to help me?
> A: PhD students should receive proper training on data protection and universities should make appropriate provision for confidential storage of data.

In spite of a disclaimer in relation to the advice provided [13], it is clear there is no accommodation of the fact that much qualitative research over the past decade no longer generates data in the form of 'piles' of paper for which a suitably locking filing cabinet provides the necessary security. Instead, we increasingly record interviews on hand-held digital voice recorders, and hold copies of transcribed interviews on both laptop and desktop computers, as well as on portable storage devices such as USB memory sticks. The lockable filing cabinet simply does not address the particular security issues generated in the digital era.

Emerging guidance on digital data security [14] does not for the most part address the particular issues of relevance to qualitative researchers [15]. These often technical contributions generally function to provide researchers with 'principles' for data security. Our approach, in contrast, translates principles into concrete strategies and procedures that researchers embarking on their research can employ. Our resulting recommendations are grounded in how we contended with the challenges of maintaining good data security practices in a team-working context, and so we pay particular attention to the problems for data security posed for researchers working in teams. In addition to discussing what we found that 'worked' for us, we discuss the procedures we had originally employed that we discovered *not* to work. It is ultimately only after a security breach that procedures are put to the test; moreover, the initial procedures we employed certainly looked good on paper: they passed through our University Research Ethics Committee, and we'd have employed them again had we not experienced the loss of data we did.

Background to the protocol

Our research involved collecting highly sensitive data in the form of interviews and fieldwork notes from gang members, former members, gang associates and others in the community. After considerable time and effort, we were finally successful in gaining the trust of key actors; we were rewarded in hearing them talk candidly over a period of more than two years about their own lives and those of others, including in relation to serious criminal events. Should these data – in the form of, for example, transcribed interviews – be made public, this could result in danger to interviewees themselves or people they discussed, from others in the community or from the police.

Our initial data security procedures, as approved by our University Research Ethics Committee (University of Manchester) in 2003, were as follows:

1. Aim to hold data digitally rather than on paper; transfer from paper (eg, fieldwork notes) as soon as practically possible.
2. Use passwords on all text versions of data (eg, interview transcripts) using available password facilities (eg, in Microsoft Word).
3. Enable log-in passwords on laptops used by fieldworkers.
4. Minimize the time data is held away from secure university premises (eg, with fieldworkers, transcribers).
5. Anonymize data as soon as possible after collection.
6. Delete non-anonymized data (eg, voice recordings) as soon as possible.
7. Back up all digitally-stored data onto transportable media (CDs, mini-disks) and store in locked filing cabinet.

Only a few months into our fieldwork, an unexpected event put our procedures to the test. A laptop containing a handful of digital voice files of recorded interviews – and their transcriptions – was stolen from the home of a fieldworker after a break-in. Our first response was to report the theft to the police and

alert our university Ethics Committee (to whom we were obliged to report unexpected events affecting ethical aspects of our research). We then set about informing each of the people with whom we had conducted the stolen interviews of the loss. We were fortunate that not one of these interviews (all had occurred early in our research) involved interviewees in discussing other people, or highly sensitive events such as those we succeeded in getting data about in later stages of our research; moreover, the names of interviewees themselves were not included in the data files. We were also fortunate that our interviewees were all unfazed by the loss, convinced that the laptop's contents were very likely to be wiped before being sold on. Finally, we set about re-thinking our security procedures. One part of our re-think involved consulting a clinical colleague, who had developed some expertise on data security in relation to data he held about his patients, along with IT staff in our own university with expertise on data security.

It is easy to be lulled into a false sense of security because of the fact that digitally-held data often incorporates straightforward and automatic protection features (eg the use of passwords) that paper-based approaches do not. We have discovered, however, that digitally-held data are just as vulnerable as paper-based versions, and are in some ways more so. For example, digitally-held data facilitates sharing data *quickly* within a research team (such as between fieldworkers and managers); this is an undeniably useful feature of the digital approach to team working. However, this in itself multiplies opportunities for insecurity. But procedures developed for a time when the qualitative research process was primarily paper-based (eg the 'locked filing cabinet'), on their own, provide insufficient security for qualitative data in a digital age. Indeed, paper versions of 'raw' data increasingly may never appear, as all operations carried out by qualitative researchers – from collecting and transcribing data, to reading and analysing it – can be now be carried out, and increasingly are carried out, on-screen only, and without ever having to print onto paper. It is therefore important to recognize that *digitally-held data does not automatically provide for 'better' security:* both digital and paper-based approaches to holding and processing qualitative research data bring with them their own security problems that need to be acknowledged when devising security procedures.

The 'principle of proliferation'

The principle of proliferation can be illustrated by counting the versions (voice files and their transcriptions as text files) and copies (identical versions of the same digital files) of an interview that can produced on its 'journey' over the course of a research project. This is illustrated in Table 1 below, with a running count of the copies that might proliferate at each turn. Of course, the number of versions and copies illustrated here is not inevitable, and to the

Table 1: The proliferation of digital data: the journey of one interview.

Activity	*Copies/versions of data files produced (cumulative)*
An interview is conducted by a fieldworker and recorded as an MP3 file on voice recorder	1
This file is later transferred to the fieldworker's laptop computer	2
This voice file, via a memory stick, is transferred to the research manager who stores the file on a university desktop computer…	3, 4
…and later transferred again, perhaps after a few interviews have accumulated, to a transcriber, again via a memory stick	5
The transcriber stores the voice file on a laptop, where it remains during the process of transcription into a text file	6, 7
The text file is transferred back to the research manager via a memory stick, where it remains on the university desktop computer	8, 9
This transcribed text file of the interview is shared in a research team meeting after it is emailed…	10, 11, 12, 13
…to all four staff members participating in the meeting, and after these team members have saved the text file of the interview to their desktop/laptop computers…	14, 15, 16, 17
…the text file of the transcribed interview is 'backed up' to protect against loss/damage	18
All transcribed interviews, including this one, are transferred to the locations in which analysis using CAQDAS by the three team members carrying out data analysis will work	19, 20, 21
Finally, once research and analysis are complete, the text file of the transcribed interview will be stored permanently and securely for future use on university premises, perhaps on a desktop or burned to a CD…	22
…and then prepared for public archive…	23
…and finally archived	24

extent that the number can be reduced, so much the better. What is certain is that as data proliferate, so do opportunities for insecurity.

Table 2 below provides an analysis of the underlying sources of proliferation for qualitative data that include its various forms (voice, text), physical locations (office, home, in the field), storage devices (voice recorders, laptops, desktops, memory sticks), individuals with particular roles on a research team (managers, fieldworkers, interviewers, transcribers), and different phases of the research (data collection, data analysis, data archive).

Guidelines for the security of digitally-held qualitative data

We developed the following guidelines to improve the security of digital qualitative data. These guidelines take into account the principle of proliferation discussed above, and what we learned from the successes and failures in the youth gang research study.

Guideline 1: Devise a written policy and revise it as required

A written policy for confidentiality and data security should be devised that is well understood by all members of the research team with access to the data [16]. The content of this policy could, for example, take some of the recommendations that follow as a starting point, with modifications to suit the particular demands on the research and its context. A member of the research team should be designated to be in charge of ensuring that data security protocols are followed. This can be part of what institutions such as the Australian National University call a 'Data Management Plan' [17]. Apart from putting in place procedures to increase the security of data, these plans may improve the efficient management of the research team and its activities through good organization, collaboration and documentation.

Guideline 2: Passwords

Passwords to protect access to files, computers and devices are useful, and should be employed; however the protection offered by many password features is flimsy (eg, 'log-in' passwords on laptop computers are relatively easy to get round). Use 'good' passwords that: combine letters and numbers, combine uppercase and lowercase characters, and are sufficiently long (security-related advice, available on the web, rarely recommends passwords shorter than 8 characters, with longer passwords even better). Use different passwords for different purposes. Do not allow your computer to 'remember' a password for you. Top-rated blog 'lifehacker' (lifehacker.com) provides daily advice on a range of productivity-related topics relevant to those working digitally, including reviews of the latest (often freeware or shareware) utilities for creating and maintaining secure passwords.

Table 2: The sources of proliferation for digital qualitative data.

1. **Digitally held data is stored in numerous locations during research.** These places include: in 'the field'; in the home of fieldworkers, interviewers, transcribers, and research managers, in the university offices of people with various roles, and 'in transit' between all these locations. *Security procedures developed for digital data must take into account the potentially numerous geographical locations in which digital data are held over the course of research.*
2. **Digitally held data is used by numerous individuals with a variety of roles on a research team.** The many forms of digital data, held in many places, are also used by a number of individuals with different roles on a research team, and can be transferred back and forth between them, for example, in preparation for, and subsequent to, team meetings in which collected data are reviewed. The relevant individuals include: interviewers, fieldworkers, transcribers, research managers, and those responsible for data analysis. *Security procedures developed for digital data must take into account that digital data is likely to be passed back and forth during the data collection and analysis phases of research between members of a research team with different roles*.
3. **Digitally-held data are stored on a number of different devices during data collection and analysis.** The devices on which digital data are held during fieldwork can include: the recording device on which voice recordings of fieldwork notes or interviews take place (increasingly, these are MP3-type recorders with in-built solid-state storage); 'smart' phones; university office and home-based desk-top computers; laptop computers; and portable digital storage devices like USB storage devices (aka thumb drives, pen drives, memory sticks) and CDs. *Security procedures developed for digital data must take into account that digital data is usually stored a number of different devices.*
4. **Digitally held data is stored in numerous versions.** These include: digitally recorded voice files (of interviews or fieldwork notes) held in MP3 format or similar; transcriptions of voice files held in word-processed documents; versions of work-processed text files held in CAQDAS (such as NVivo and Atlas.ti). *Security procedures developed for digital data must take into account that data are held in a number of versions including voice files, text files for holding transcripts and notes, and text files for use in data analysis software (CAQDAS).*
5. **Digital data are held over a range of times coinciding with the various phases of qualitative research.** These times or phases of the research process during which digital data are first collected and then manipulated and held include: initial data collection, adding to collected data, storing collected data, analysing data, and then finally, more long term archiving of collected data. *Security procedures developed for digital data must take into account the different phases of research and the length of time that data are required to be held.*

Guideline 3: Encryption

Use encryption software to create 'encrypted space' on computers and storage media (like USB portable memory drives/sticks) for all research data, or to encrypt individual files. A number of different approaches to encryption of text-based data are available, including commercial varieties and free open-source software like TrueCrypt and AxCrypt. Use of encryption software means that, in the event of loss or theft of a device, it becomes extremely difficult for someone to access the encrypted files. Files can be moved back and forth between encrypted and non-encrypted storage, and even be emailed as attachments, helping to facilitate group working in a relatively secure way.

Guideline 4: Managing the storage and deletion of data

Research managers not only need to manage the process of data collection by fieldworkers, but also its storage (and deletion) by all who come into contact with the data. Simply asking fieldworkers to delete permanently digital data files (for example, voice recordings) once transferred to the central research location does not guarantee this will actually happen (and to be fair, many of us are not always on top of these kinds of 'housekeeping' activities). Put in place management strategies (and ensure these are documented – see Guideline 1) to check regularly that fieldworkers follow security protocols. Insist that all people who will be dealing with your research data, including those not directly employed by your institution, use security procedures at least as good as the ones you employ. Transcription work is sometimes contracted out to external companies. Do not assume their security procedures are sufficient: ask them to demonstrate their procedures, and ask if they are willing to adopt your procedures for the work they do for you.

Guideline 5: Making back-ups

Make back-ups of data from encrypted computer disks only to portable media (eg USB memory drives) that have been encrypted and store/carry these separately. Where the only two copies of data (eg, laptop and USB memory stick) are being transported together (eg, digital coding work being transported daily between work and home) the laptop and memory stick should be carried separately (ie, not all in one bag) in case of loss or theft. Even though, in the event of loss, data stored on the encrypted portions of these devices may not be easily recovered by others, the loss of work (for example, during the coding process) is undoubtedly detrimental to the research project.

Guideline 6: Security in the field

Employ the style of field note taking (on paper, or digitally via voice or text files) that is most suitable to the research and that suits personal preferences; however, delete and permanently destroy notes held temporarily in any medium that is not encrypted (paper notes, voice recording) as soon as possible, and in preference for more permanent encrypted storage away from the field setting.

Guideline 7: 'On screen' working methods

Employ on-screen methods for reading and analysing data if possible. However, even researchers adopting primarily digital methods sometimes prefer not to carry out some tasks on screen, such as reading transcripts, comparing documents, or for discussion reference in meetings. When paper copies of data are produced, these should be shredded (using a cross-cutting shredder) immediately after use, in preference to storing them.

Guideline 8: Deleting data

Simply deleting files from a computer's hard disk does not remove them permanently. Employ methods to delete files permanently and completely so that they cannot be recovered. 'Clean' the spaces on the disk from where files have been deleted. Permanently remove the 'temporary' files (essentially copies) that various programmes (such as word processors) create. Various software products are available to accomplish this kind of clean-up work (for example, AbsoluteShield Field Shredder, CleanUp, Steganos Privacy Suite). This is important because computers can often be sold on or recycled within research institutions without this information having been permanently deleted [18].

Guideline 9: Sharing data via email

Sharing data documents by attaching them to emails is useful for team-working. Never send non-encrypted confidential data by email – even if you save the attached file securely and then immediately delete the original email – because even deleted emails and their attachments can be recovered from email servers. Ensure that only encrypted documents are shared by email.

Guideline 10: Former employees

Former employees may retain possession of or access to data once their employment has ceased. Put agreements in place with those employed to work with data (eg, fieldworkers, transcribers) requiring these individuals to return data and media on which they are stored when they no longer require access, alongside 'good practice' activities such as 'deep cleaning' hard disks that remain in their possession when data have been deleted (see Guideline 8). It is important to ensure that these activities occur when contact with the employee is still in place. Another useful strategy is to change passwords that grant access to data that are held communally (see Guideline 13) once the need for that access is finished.

Guideline 11: Tracker software

In the event of loss or theft, tools are available to allow lost or stolen computing equipment (such as laptops or 'smart phones') to be traced and tracked down (eg Adeona, LoJack and GadgetTrak). Smart phones such as Apple's iPhone and the Blackberry (alongside the many others similar to these on the market) can be particularly handy for researchers, allowing them to record interviews, encrypt files, and even place them in secure locations for sharing (see Guideline 13). In the event of loss or theft of these hand-held devices, some services make it possible to issue a remote command (eg Apple's 'MobileMe') to wipe the data contained on a smart phone. However, none of these strategies should be seen as a replacement for encryption (see Guideline 3).

Guideline 12: Anonymization

Early anonymization of interview transcripts and fieldwork notes is always the ideal; if anonymized transcripts are lost or stolen, problems in relation to confidentiality are minimised. Each name, place, and organization should be replaced with unique identifiers (eg, a pseudonym), rather than anonymous placeholders (eg, 'Person Name'). Without this, ongoing analysis is compromised by loss of meaning as the links between individual names are severed. However, 'unique identifier' anonymization may be impossible at an early stage. In our research, interviewees spent considerable time talking about other known individuals, eventually numbering in their hundreds, and working out 'who was who', particularly given the proliferation of nick-names and street names, was difficult at the start – indeed, the process was never complete.

Guideline 13: Storing data centrally rather than locally

Many of our guidelines (above) are aimed at researchers who create and store data on local machines (ie PCs, laptops and the like) and transfer resulting data files from one location/device to another using portable memory media (eg USB memory sticks). Increasingly, in both the business and public spheres, there is a move towards the secure storage of data in central locations that can be accessed by multiple users in remote locations. 'Cloud' computing, in which data files or software are located on the internet and then simply accessed via local machines, is also becoming popular. These kinds of developments are significant for researchers concerned about data security because they reduce the production of multiple copies of data that result when working digitally, and especially in a team working context.

A Virtual Private Network (VPN) for example, creates an encrypted connection between a remote machine (such as a laptop used from home) and a central server (such as your university's server). A VPN therefore provides the means to communicate private information securely over a public network. The proliferation of hand-held devices that can be used simultaneously for recording of interviews, note taking and internet use has dramatically increased since we completed our research project and their technical specifications for these purposes are likely to improve in coming years. Many of these devices, including iPhones and other 'smart phones', allow for the configuration of VPNs. Alongside VPNs, applications such as Microsoft's SharePoint can be used for the central management of your data. 'Sharepoint' incorporates encrypted SSL certificates, which means the data in transit from computer to the server is also encrypted and only those with approved access can log in to access the data.

The use of centralised storage facilitated through internet connections like those we've just described carry with them different security risks to those posed by storage on local computers and portable media. The appeal, however, lies in how their use allows us to address the problem of 'proliferation' of digital data by reducing or eliminating the need for security-problematic multiple copies of data. VPNs and secure web-based document sharing software can also be used to facilitate the sharing of data important to team working by allowing remote access – again reducing the problem of proliferation. It is important to highlight that not all forms of central data storage are equally robust. For example, encryption is not enabled by default to protect information transmitted by users of Google Docs [19] (another cloud computing innovation) and, as a result, Google customers who compose documents from a public connection face a very real risk of data theft and snooping. The commercial providers of various cloud computing innovations say little about the confidentiality or privacy of the information placed under their control, and the legal rights and regulatory authority for the protection of the privacy of cloud computing users are not well defined [20].

Guideline 14: Data security in the public archive

The problems of data security continue beyond data collection and analysis into the final stages of data archive. If interview data pose confidentiality problems that prevent them being publically archived (for example, where extensive anonymization results in impoverished or misleading data, as was the case in our youth gangs research), consider putting in place the possibility for individually negotiated agreements allowing other researchers to access data in order to facilitate secondary analysis and comparative research. If interview transcripts or other data containing identifying information are not anonymized at the point of

creation or before, sensitive information in these files must be 'redacted' (blacked out). Our first strategy for redacting identifying text in interview transcripts did not destroy the text, but created only temporary invisibility by making the text and the background the same colour. Our second strategy involved replacing selected text with placeholders like 'XXXX'. We learned, however, that word-processing programmes contain hidden code that can later be used to reveal previous versions of the document, thus making it possible to uncover deleted information, and providing a further threat to anonymity and security when these documents are shared or archived. Commercially-available solutions for digital redaction are available, and more thoroughgoing but time-consuming approaches involve copying redacted documents into 'text only' documents that are stripped of hidden code, and then removing and permanently deleting 'temporary' files created by the word-processor. Guidance provided by the National Security Agency of the United States provides step-by-step guidance for redacting text in documents [21].

Concluding remarks

We consider these guidelines to be necessary – but not necessarily sufficient – conditions for the security of digitally-held data typically produced by qualitative social researchers. However, the information and communication world is a fast-changing one, and new security issues in relation to digital data arise constantly. Our approach has been to translate often abstract data security principles into concrete suggestions for practice that researchers can employ. We welcome improvements and additions to our guidelines. No doubt our own practices in this regard will evolve quickly as technology – and the problems and solutions it creates – evolves alongside them.

Acknowledgements

Our appreciation goes to John Churcher, who took the time to get to know our project and our data security needs. His knowledge and assistance were key to helping us develop our guidelines.

References and notes

1. UK's families put on fraud alert. BBC News, 2007. Retrieved from http://news.bbc.co.uk/1/hi/7103566.stm at 3 February 2010.
2. Although one of the more high profile losses of data, this is not the only loss of data by public organizations in the UK. The Open Rights Group (ORG) is a non-governmental organization that raises awareness of issues such as privacy, identity, and data protection. A wiki produced by ORG includes a page devoted specifically to 'UK Privacy Debacles' enumerating data losses by public organizations. Between 24 April 2009 and 29 October 2009 alone, the loss of 878 513 records by 35 organizations is listed. Included in the list is the University of Manchester, after a member of staff emailed an attachment to 469 students with data on 1700 people including information on student disabilities; and Imperial College when six laptops were stolen resulting the loss of medical data containing confidential information on 6000 patients. UK Privacy Debacles. Open Rights Group. Retrieved 3 February 2010, from http://wiki.openrightsgroup.org/wiki/UK_Privacy_Debacles.
3. Thomas R. Evidence to the Justice Select Committee, 2009. Wilmslow, Information Commissioner's Office.
4. Aldridge J, Medina J. Youth gangs in an English city: social exclusion, drugs and violence. Final report to the ESRC, 2008.
5. Aldridge J, Medina J, Ralphs R. Dangers and problems of doing 'gang' research in the UK. In: Street gangs, migration and ethnicity. Ed. van Gemert F, Peterson D, Lien I-L. Cullompton: Willan Publishing, 2008: 31-46.
6. Aldridge J, Shute J, Ralphs R, Medina J. Blame the parents? Challenges for parent-focussed programmes for families of gang-involved young people. Children and Society, 2009.(DOI: 10.1111/j.1099-0860.2009.00282.x).
7. Ralphs R, Medina J, Aldridge J. Who needs enemies with friends like these? The importance of place for young people living in known gang areas. J Youth Studies 2009; 12 (5): 483-500.
8. Aldridge J, Ralphs R, Medina J. Collateral damage: territory and policing in an English gang city. In: Youth in crisis? 'Gangs', territoriality and violence ed Goldson B. Cullompton: Willan Publishing, 2010.
9. Medina J, Aldridge J, Ralphs R. Gang transformation, changes or demise: evidence from an English gang city. In: Global gangs: comparative perspectives ed Hazen JM, Rodgers D. Minneapolis: University of Minnesota Press, 2010.
10. Medina J, Ralphs R, Aldridge J. Mentoring siblings of gang members: a template for reaching families of gang members? Children and Society, in press, forthcoming 2010.
11. Code of Ethics and Policies and Procedures of the ASA Committee on Professional Ethics. American Sociological Association. New York, American Sociological Association, 1999.
12. Code of Ethics for Researchers in the Field of Criminology. British Society of Criminology, 2006. Retrieved from http://www.britsoccrim.org/ethical.htm at 3 February 2010.
13. The British Society of Criminology states that the questions and answers listed in their guidance are 'intended to provoke thought and debate: the answers given are not to be taken as definitive.' Ibid.
14. RELU Data Support Services. Guidance on Data Management. Colchester, UK Data Archive, University of Essex, 2006.
15. Although for a discussion of some of these, see Corti L. Data security. The SAGE Encyclopedia of Qualitative Research Methods. Given LM. London: Sage, 2008.
16. Brady HE, Grand SA, Powell MA, Schink W. Access and confidentiality issues with administrative data. In: Studies of welfare populations: data collection and research issues ed Ver Ploeg M, Moffitt RA, Citro CF. Washington DC, National Academy Press, 2002: 220–274.
17. Australian National University Data Management Manual: Managing Digital Research Data at the Australian National University. Canberra, Australian National University, 2008.
18. Jones A, Valli C, Dardick GS, Sutherland I. The 2007 analysis of information remaining on disks offered for sale on the second hand market. Int J Liability Scient Enquiry 2009; 2(1): 53-68.
19. In January 2010, Google made changes to its googlemail/gmail service so that browser connections are now encrypted via SSL by default. This action followed a letter sent to Google CEO by leading academics and security specialists requesting encryption on all Google services by default (Letter to Eric Schmidt, CEO Google inc., from (Appelbaum and and 37 others June 16 2009. Available at http://epic.org/privacy/cloudcomputing/). However, Google Docs, at the time of writing, remains unencrypted by default.
20. For details see Electronic Privacy Information Centre at http://epic.org
21. Redacting with confidence: how to safely publish sanitized reports converted from Word to PDF. Ft. Meade, National Security Agency, 2005.