Caring for Data:
Law, Professional Codes and the Negotiation of Confidentiality in Australian Criminological Research.

Final Report

Robert Chalmers, School of Law,
University of Adelaide

Mark Israel, School of Law,
Flinders University

January 2005

Authors

Robert Chalmers *is a Lecturer in the School of Law at the University of Adelaide and a Commercial Development Manager at Adelaide Research and Innovation Pty Ltd. He has experience as a legal practitioner and government advisor in relation to confidentiality and privacy law, providing advice on over 400 confidentiality agreements in the government and corporate sector. He has practised as a lawyer in the field of intellectual property law since 1990 working with the Australian Government Solicitor, CSIRO, DSTO and the commercial law firm Norman Waterhouse. Since 1992, he has provided advice on policy development and extensive training on risk management in relation to confidentiality and privacy laws to the research divisions and management of Commonwealth government research agencies and departments as well as to the South Australian Attorney-General's Department and the University of Adelaide. Views expressed in this paper are made in an academic capacity.*

Mark Israel *is professor of criminology in the School of Law at Flinders University where he is also Associate Dean (Research). He has qualifications in criminology, sociology and law. He is author, co-author or editor of over 50 books and articles on topics as diverse as South African Political Exile in the United Kingdom (Macmillan 1999), Criminal Justice in Diverse Communities (Federation 2001), Crime and Justice in Australia (Lawbook Company 2003), victimology, jury selection, coverage of crime by the media, community corrections and state crime. In 2004, he published an article on confidentiality in criminological and socio-legal research in the British Journal of Criminology and completed a report for the New South Wales Bureau of Crime Statistics and Research on Ethics and the Governance of Criminological Research in Australia. His book, Research Ethics for Social Scientists, co-authored with Iain Hay will be published by Sage in 2006. This report for the Criminology Research Council draws on and develops some of the material in that body of work.*

Summary

In this report, we offer guidance to criminologists attempting to navigate, and manage the impact of, laws that relate to the protection and disclosure of confidential and personal information that they gather in the course of their research.

We start by providing examples of the impact of relevant laws on the practice of criminologists to set this work in it proper context, and then provide a general overview of laws relating to issues such as privacy, confidentiality and compelled disclosure. Drawing on this background, Section Three provides brief responses to Frequently Asked Questions covering the ways researchers gather, store, use, disclose and reuse information. We conclude by examining possible future developments.

Throughout the report we attempt to illustrate how the practice of criminological research practically intersects with relevant laws. This intersection can be painful as relevant laws are by no means tailored to suit the environment of such research. However, our aim is to help criminologists and their institutions reach better informed decisions about management of legal risks although, of course, this report is not a substitute for specific advice.

Acknowledgments

We wish to thank the Criminology Research Council for funding this research, Andrew Stewart of Flinders University and Martin D. Schwartz of Ohio University for acting as consultants and Alice Faunce-de Laune for help with research and editing. Parts of Section One of this report are drawn from Israel and Hay (2006) *Research Ethics for Social Scientists* and appear in this report courtesy of Sage Publications. Thank you also to our families for giving us time away from domestic duties to complete the report.

Abbreviations

ANZSoC	Australian and New Zealand Society of Criminology
ARC	Australian Research Council
ASIC	Australian Securities and Investment Commission
ASIO	Australian Security Intelligence Organisation
AVCC	Australian Vice-Chancellors' Committee
CRC	Criminology Research Council
HREC	Human Research Ethics Committee
IPP	Information Privacy Principles
NHMRC	National Health and Medical Research Council

Introduction

Criminological research often involves handling data relating to illegal or sensitive activities. Researchers may need to negotiate the way they use this data with a range of parties, including research participants, funders, clients, government agencies, and regulators of law and ethics. They do so in an uncertain legal environment and in the face of considerable recent change at statute and common law. This uncertainty has had several consequences.

First, criminologists have been exhorted by their professional organisations and employers to develop an understanding of the legal regulations that govern their research. So, section five of the Australian and New Zealand Society of Criminology Code makes references to respecting undertakings of confidentiality and requires members to 'comply with all legal requirements' (Australian and New Zealand Society of Criminology Code s.5a). These sentiments are reiterated in the various national ethics codes such as the National Statement on Ethical Conduct in Research involving Humans (1999) and the Draft Australian Code for Conducting Research (National Health and Medical Research Council et al. 2004). For example, the first consultation draft of the National Statement on Ethical Conduct in Research involving Humans (2004) warned that 'It is the responsibility of institutions and researchers to conform to both general and specific legal obligations, wherever relevant.' (p.4).

A review of ethical governance of criminology for the New South Wales Government completed by Mark Israel (2004b), one of the authors of this report, pointed to the need for criminologists to improve their knowledge of laws relating to confidentiality and privacy. However, considerable work needs to be done to provide Australian criminologists – including those who possess legal qualifications – with the means to do so and, for the most part, this has not happened, leaving government-, university- and private-based researchers and their host institutions vulnerable.

Second, various government and research institutions have been developing risk management practices for sensitive data. However, these policies have not always been responsive to the problems associated with criminological research.

Criminal and civil liability in drug research

One successful attempt to provide the appropriate legal background for criminological research occurred when the National Centre for Epidemiology and Population Health and the Australian Institute of Criminology commissioned legal research to review the potential criminal and civil liability in drug research associated with a heroin trial in the Australian Capital Territory (Cica 1994; Bronitt 1995).

Section One of this report reviews the occasions when criminologists and other researchers have faced legal difficulties as they have sought to protect confidentiality, gain access to or release data. Parts of this section have already been or are about to be published elsewhere (Israel 2004a, 2004b; Israel and Hay 2006), and draw on both Australian and North American experiences. In Section Two, we provide a general overview of laws affecting the gathering, storage, use and dissemination of research material reviewing laws relating to confidentiality, privacy, compelled disclosure, freedom of information, archives and mandatory notification. This provides a basic understanding of the legal environment within which criminologists operate. In Section Three, we identify common issues of concern for researchers and the specific impact of key legal obligations on the running of research projects. We also propose strategies for managing these obligations and attendant risks. The report concludes by considering some of the likely future legal developments.

This report has been written by a criminologist, Mark Israel, with a disciplinary background as a sociologist – albeit one with a rather under-exercised law degree – and a lawyer, Robert Chalmers, with extensive experience advising Australian university- and government-based researchers about laws relating to information management. The division of labour was fairly straightforward – the criminologist identified the problems faced by researchers and posed questions to the lawyer. The lawyer attempted to answer in a way that made sense to the criminologist. The criminologist kept asking the lawyer until he believed that he did.

Several disclaimers normally follow legal advice. The law covered in this report reflects the situation in January 2005. We are covering a lot of ground over multiple jurisdictions and have deliberately avoided some legal jargon and considerable technical detail. As a result, this report is probably best used as an overview or a guide. Researchers would be well advised to check the detailed

provisions of their own jurisdictions and, where necessary, seek their own legal advice.

Section One: Criminologists, their Data and the Law

When people allow criminologists to investigate them, they often negotiate terms for the agreement. Participants in research may, for example, consent on the basis that the information obtained about them will be used only by the researchers and only in particular ways. The information is private and is voluntarily offered to the researcher in confidence. Researchers can justify protecting confidentiality by appealing to consequentialist- (O'Neil 1996; Fitzgerald and Hamilton 1997; Van Maanen 1983), rights- (Allen 1997; Beauchamp and Childress 2001) or fidelity-based (Bok 1983) arguments. Failure to respect confidentiality might not only affect one research project but could have a 'chilling effect' on all criminological research (McLaughlin 1999). Consequently, in general, criminologists try to respect confidences although they may be vulnerable to pressure from courts and law enforcement agencies to disclose confidential material. This may be a growing problem as the number of agencies with powers to obtain such data has increased over the last few years.

While criminologists have paid some attention to the question of confidentiality, matters relating to privacy have been largely ignored. Yet, issues concerning privacy arise when criminologists obtain secondary data from government agencies or other organisations or share material with other researchers. In these cases, the law places considerable and often quite complex restrictions on researchers' access to and use of data.

This section is based on Israel (2004a, 2004b) and examines those occasions when criminological researchers have faced ethical difficulties in complying or resisting legal requirements to disclose or protect information given to them by research participants.

Negotiating access to confidential data

Constraints by privacy legislation and policies on access to data are a major disincentive to establishing and maintaining longitudinal studies and using potentially valuable existing data sets. The National Statement stipulates that generally the consent of participants should be obtained for using their personal information by those or other researchers in future projects (NS 18.4), although this seems not to be an absolute requirement. Epidemiological research has the same stipulation. However, ethics committees can approve access without

consent, subject to an overriding public interest in the research, on one of three grounds: if it is impossible in practice to obtain consent, or gaining consent would pose some risk to the people who would be approached, or prejudice the scientific value of the research (NS 14.4).

The usual scenario is one where data collected, possibly some time ago, by a researcher who had consent for one purpose could be re-analysed to provide other valuable insights, perhaps into research questions that were not apparent when the data was originally collected. The participants are identifiable, though this is not necessary for the proposed new research. For very large population data sets, seeking consent would be prohibitively expensive or impractical. The costs for the data-holder in de-identifying can be similarly prohibitive. Even so, many research ethics committees are reluctant to approve proposals to use data in these circumstances, though the risk of harm may be minimal, and the potential benefits could be significant.

Similar privacy considerations apply to research using data linkage. Access to identifying information is essential for analysis from different data sets, for longitudinal studies where participants are interviewed more than once over an extended period of time, or where different variables are analysed as they become available. While technological advances make such research increasingly possible, current privacy legislation and codes make it increasingly difficult. Personal information may only be used to allow records to be linked without the consent of participants if a researcher obtains the approval of a research ethics committee. The committee must be satisfied that personal information will be disclosed only for the purposes of linkage, will not be retained once linkage completed, will be done with sufficient security. The committee must also conclude that the research has public benefit (NS 18.5).

Researchers and agencies find it difficult to interpret complex and evolving privacy laws that operate according to different state and federal regimes and vary in impact depending on the source of the data. Different regimes make nationwide research more complex to design and conduct and less reliable where data are not comparable.

Negotiating the release of confidential information

As we shall discuss, both Bok (1983) and Beauchamp and Childress (2001) concluded that obligations of confidentiality were only *prima facie* binding. This

means that they cannot be considered absolute and in some situations researchers should contemplate disclosing to a particular person or group information that they had received under an implied or explicit assurance of confidentiality. So, while many researchers have sought to avoid releasing confidential information, there are some situations where researchers have argued that it would be appropriate to breach confidentiality.

In the field of bioethics, Beauchamp and Childress (2001) developed a starting point for assessing whether to infringe obligations of confidentiality on the basis of possible consequences of a failure to disclose. Focussing predominantly on risks to third parties, they argued that the weight of the obligation to breach confidentiality increased as the probability and magnitude of harm increased. In borderline cases, they suggested that researchers consider the foreseeability of a harm, the preventability of the harm through the intervention of the professional (presumably interventions that did not require a breach of confidentiality), and the potential impact of disclosure. Of course, they recognised that 'Our attempts to measure probability and magnitude of harm are imprecise in many cases, and uncertainty will be present.' (Beauchamp and Childress 2001: 309).

The 1997 American Sociological Association's Code of Ethics allows researchers to consider breaching confidentiality if, in unanticipated circumstances, they received information about clear and prospective, serious harm (s.11.02(b)). Serious harm is defined as life- or health-threatening. Lowman and Palys (2000) argued that in such cases of 'heinous discovery', researchers should distinguish between the kinds of serious harm that they could anticipate discovering during a particular piece of research and those that they could not. In the first instance, Lowman and Palys argued that researchers had two options. They should either be prepared to hear about such activities and keep quiet, or shoudl not undertake the research (see also Wolfgang 1981, Norris 1993).

Lowman and Palys acknowledged that sometimes researchers discovered information about serious future harms or past injustices that had nothing to do with their current research. This, they maintained, was information that they would be prepared to divulge while ensuring the safety of all parties and minimising the extent to which the confidence would be breached. As a result, Lowman and Palys described the assurance that they would give research participants as 'unlimited' as opposed to 'absolute'.[1]

[1] Private Communication from John Lowman to Mark Israel, 23 February 2003.

Lowman and Palys' position on this point is consistent with that of Sissela Bok. Bok (1983) argued that people who provided information in confidence could not expect to maintain their right to secrecy if they acted in bad faith by, for example, intending to harm a third party. In the context of HIV transmission, Gillett (1987) termed such reliance as 'moral free-loading'. Bok suggested that someone who knew of the potential harm could act to counteract the plan or, failing that, warn the potential victim as long as the confidence was violated only to the extent necessary to forestall the harm. For Bok (1983), when considering whether to breach a promise, researchers must consider whether it was right to make or accept the promise in the first place, whether the promise was or is binding, and under what circumstances it might be justifiable to override it.

When researchers decide that promises of confidentiality are not binding, they *may* be in a position to disclose information. However, this is a long way from saying that they *must* disclose.

Resisting pressure to breach confidentiality

Threats to the confidentiality of data gathered by researchers may be rare but they are not so uncommon that they can be ignored by researchers. Researchers have come under pressure from various criminal justice agencies, including the police and the courts to divulge information. The clearest Australian example involved Fitzgerald and Hamilton's (1996) work on illicit drug use in Australia which was compromised when one researcher was approached by a police officer working undercover.

> The undercover police officer suggested that a trade of information could be done: the undercover officer would introduce the ethnographer to drug users to interview in exchange for information that the ethnographer could pass on to the police. (p.1593)

Fearing police might seek access to their data by getting a warrant or by placing fieldworkers under surveillance, the researchers suspended their fieldwork while they sought to clarify their legal position.

Several other instances of legal threats to the confidentiality of research data can be found in North America. For example, although criminologists and socio-legal scholars were not involved, fishing expeditions for research data were conducted

by American manufacturers subject to lawsuits involving the drug diethylstilbestrol (DES),[2] tobacco[3] and the Copper Seven intrauterine device.[4] In the latter case, attorneys demanded 300,000 pages of documents from a non-profit institute that had undertaken research in the area (Wiggins and McKenna 1996). More recently, ten American universities received subpoenas from tobacco companies demanding thousands of documents from studies conducted in the previous 50 years (McMurtrie 2002).

Social scientists *have* refused to reveal information to government investigators (James 1972; Kershaw and Fair 1976; Maisel and Stone 1998) or to courts (Gillis 1992; McNabb 1995; Picou 1996; O'Neil 1996; McLaughlin 1999; McCollum 1999; Wilson 2003).[5] As the following examples illustrate, the reasons for their decisions and the point at which they decided they could no longer co-operate with the legal system vary considerably.

In 1974, a Californian graduate student observing police patrols witnessed a police assault of a civilian (Van Maanen 1983). Although Van Maanen gave police internal investigators a sworn statement about the incident, the patrol officers were exonerated. The police officers sued a newspaper that covered the assault. When the paper subpoenaed Van Maanen's field notes, he refused to show them. Van Maanen decided that while he would be willing to testify about the assault, he was not prepared to hand over notes that contained '...raw details about questionable, irregular, and illegal police actions with the names of those involved...' (1983: 275). Fortunately for Van Maanen, the officers' case was dismissed before the researcher had to face potential consequences for his decision.

In the 1980s, a New York student engaged in an ethnography of Long Island restaurants was subpoenaed together with his field notes by prosecutors investigating arson in a restaurant (Brajuha and Hallowell 1986).[6] A letter written by John Lofland, Chair of the American Sociological Association's Committee on Professional Ethics, was cited in court by the American Sociological Association, the American Political Science Association and the

---

2 *Deitchman v E.R. Squibb and Sons,* 740 F.2d 556 (7th Cir. 1984).

3 See *In re R.J. Reynolds Tobacco Co.*, 518 N.Y.S.2d 729 (Sup. Ct. 1987); *R.J. Reynolds Tobacco Co. v Fischer*, 427 S.E.2d 810 (1993).

4 *Anker v G.D. Searle and Co.*, 126 F.R.D. 515 (M.D.N.C. 1989).

5 See also *Richards of Rockford v Pacific Gas and Electric*, 71 F.R.D. 388 (N.D. Cal. 1976); *In re the Exxon Valdez* Re: All Cases, Misc. 92-0072 RV-C. (S.D. Ala. 1993).

6 *In re Grand Jury Subpoena*, 583 F. Supp. 991 (E.D.N.Y.), *rev'd*, 750 F.2d 223 (2d Cir. 1984).

American Anthropological Association. Lofland asserted the importance of maintaining the confidences of sources in a field study:

> Ethically, social scientists have desired not to harm people who have been kind enough to make them privy to their lives. At the level of sheer civility, indeed, it is rankly ungracious to expose to public view personally identified and inconvenient facts on people who have trusted one enough to provide such facts! Strategically, fieldwork itself would become for all practical purposes impossible if fieldworkers routinely aired their raw data – their fieldnotes – without protecting the people studied. Quite simply, no one would trust them...[7]

The student, Mario Brajuha, was able to maintain his promises of confidentiality by negotiating with prosecutors to remove the names of informants from sensitive material, but not before a lengthy and expensive court battle which resulted in Brajuha losing his money, his family and his desire to work in sociology.

In the late 1980s, Kenneth Tunnell and Terry Cox, two Kentucky-based researchers, were investigating a murder case when defence attorneys attempted to block their research. Threatening legal action, the lawyers demanded the researchers' field notes, interview transcripts and the names of informants. Tunnell and his colleague '...decided simply to lie and tell the attorneys that, due to their threats, we had destroyed the tapes and transcripts in question... We believed a good poker face would conceal our nervousness' (Tunnell 1998: 211). The lawyers dropped their demands.

In 1972, a Harvard political scientist, Samuel Popkin, failed to disclose to an American grand jury the names of and the data provided by government officials who had discussed a classified American Defense Department project with him (Carroll and Knerr 1973). Popkin spent eight days in jail.[8] In 1993, an American sociology graduate student, Rik Scarce, spent 159 days in jail in Washington State for contempt of court (Scarce 1999).[9] Scarce had failed to comply with a demand from a grand jury that he disclose information gathered during research concerning radical animal rights activism.

---

7 Amici Curiae Brief of the American Sociological Association, American Political Science Association, and Anthropological Association (2d Cir. 1984) (No. 84-6146), at app. 1. Cited in Wiggins and McKenna (1996: 82).

8 *United States v Doe (In re Popkin)*, 460 F.2d 328 (1st Cir. 1972).

9 *Scarce v United States*, 5 F.3d 397, 399-400 (9th Cir. 1993).

In the only case where a Canadian criminologist has been charged with contempt for failing to disclose confidential information relating to the identities of research participants (Palys and Lowman 2000), a Masters' student investigating the deaths of AIDS patients was subpoenaed by the Vancouver Coroner to appear at an inquest.[10] In his interviews with people who had assisted in the suicides, Russel Ogden had offered absolute confidentiality following a procedure approved by his university's ethics committee. Ogden agreed to discuss his research findings with the court but refused to divulge the names of research participants. Ogden met additional difficulties negotiating confidentiality when he attempted to extend his research as a doctoral student in the United Kingdom (Dickson 1999; Farrar 1999a; 1999b). In 2003, Ogden ran into further trouble when as an independent researcher he received a subpoena to appear as a prosecution witness in the preliminary hearing of a British Columbian woman charged with counselling, aiding and abetting suicide. Palys and Lowman (2003) once again argued that the subpoena would disrupt Ogden's longitudinal research on non-physician assisted suicide.

As one anthropologist acknowledged, 'The prospect of having to refuse to respond to a subpoena or to testify clearly chills the depth of researchers' inquiries' (McLaughlin 1999: 934). Although most of the examples that we have discussed are not Australian, as Lorraine Beyer observed, Australian researchers are not immune from the threat of orders from law enforcement bodies and courts to disclose information:

> In Australia, no research into illegal behaviours is immune from the possibility of... research material being subpoenaed. Thus, researchers studying... illegal behaviours must conduct their research under conflicting ethical obligations. On the one hand they must fulfil university and other professional body standards and protocols in relation to safeguarding the confidentiality of research subjects, and on the other they are legally obliged, if subpoenaed, to disclose all research information, including identifying information, to law enforcement. Lack of legislative protection leaves not only the participants vulnerable but also the criminological researchers who may be open to prosecution and jail terms in some instances, for failure to disclose material or knowledge of offences obtained by them in the course of their research. (Beyer 2003)

[10] *Inquest of Unknown Female* (1994) Vancouver Coroner Case File 91-240-0838. Cited in Palys and Lowman (2002).

Section Two: Laws Relating to Research Material

A range of laws may have an impact on the practice of criminological research. These include the common law relating to confidentiality and statute-based privacy laws, along with general laws that can be used to compel disclosure of information. In this section, we briefly discuss the nature of the obligations that flow from these laws before returning to the specific implications for criminological research in Section Three.

Laws relating to Confidentiality

While laws relating to confidentiality might be more commonly associated with commercial in confidence material or trade secrets, they are equally applicable to confidential personal information such as that gathered by criminological researchers.[11] In Australia, confidentiality obligations are primarily derived from the common law relating to the tort of breach of confidence, rather than being based in statute. There are also some statutory provisions such as the tax, medical, social security and national security-related legislation that do restrict access to or use of certain types of information but, with the exception of the *Epidemiological Studies (Confidentiality) Acts* of the Commonwealth and the Australian Capital Territory, they will not be considered further in this part of the report.

If a research participant discloses confidential information to a criminologist then, even if there is no written or explicit oral agreement between the parties that the information will be treated in confidence, the researcher is obliged to honour that confidence. Information does not have to be in material form to be protected by the common law, as long as it is sufficiently identifiable.

The case of *Coco v Clark* (1969) RPC 41 set out three basic factors that are usually required to establish liability:

- the information must have 'the necessary quality of confidence';
- the information must have been communicated in circumstances that would impose an obligation of confidence (this relies on a 'reasonable person test' – if a 'reasonable person' receiving the information in the relevant

[11] See eg *Stephens v Avery* (1988) 11 IPR 439.

circumstances would have realised it to be confidential, that is sufficient). So, the obligation does not have to be made expressly; and,

- there must be an actual or threatened unauthorised use of that information to the detriment of the party who originally communicated it.

A research participant is entitled to take action to stop the unauthorised and unlawful use or disclosure of confidential information obtained by a researcher. In addition, a participant can take action against any third party recipients of such information, as anyone who receives confidential information from another person who has breached confidence can be restrained from using or disclosing the information once they have knowledge (actual or constructive) that the information is confidential and its use is not authorised.[12]

However, obligations of confidence are not absolute. Certain defences and exceptions may apply, and courts and other agencies have special powers to compel disclosure of information. As commentary in the Human Research Ethics Handbook developed for the National Health and Medical Research Council (2001) observes, it can be difficult to maintain confidentiality when carrying out some qualitative research that might involve in depth face to face interviews (as such interviews are not truly anonymous even where identifying information is not recorded). Consequently, researchers need to be aware of the difficulties of offering participants absolute confidentiality (Israel 2004a). The Handbook declares that:

> …if legally required to testify in court researchers must do so and mandatory reporting of information that has been revealed by a participant may be required. In addition, the law does not necessarily protect 'field notes' and researchers need to be particularly careful about what they record and how this information is stored. (E131-2)

Defences

Clearly, a researcher can release confidential information if consent has been granted by a participant. In addition, even if a participant does not want information released, some disclosures in breach of confidence may be 'justified' and excused.[13] In particular, obligations of confidence in relation to illegal acts

12 *Fraser v Evans* (1969) 1 QB 349.

13 *Fraser v Evans* (1969) 1 QB 349.

or misconduct will not be enforced.[14] This might be particularly important in instances of 'heinous discovery'. However, it would be extremely awkward for future researchers if criminologists routinely relied on such a defence in breach of an obligation of confidence to a participant. We would be saying to research participants: 'I am a criminologist, undertaking research on criminal activities. I promise to keep information that you provide confidential, unless it relates to illegal acts.'

Alternatively, a breach of confidence may be excused where the public interest in publication outweighs the public interest in confidentiality. However, this requires a matter of real importance, not prurient interest.[15] It is an open question as to how broadly this defence would be applied in Australia. While it would be safest to use disclosure to the 'proper authorities' as a first step (Cica 1994; McKeough and Stewart 2002), ultimately a whistleblower may be justified in going public on a matter of public interest.[16]

Confidentiality Agreements and Provisions

People exchanging confidential information often use contracts to supplement the laws relating to confidential information and to specify the information that will be subject to defined obligations of confidence. In research projects, researchers may provide specific undertakings about confidentiality. These may be provided either orally or written into a consent form or a research agreement or even a research funding contract. Such undertakings may become relevant if a researcher wants to use the law to resist subpoena actions or restrict the scope of use of information that he or she is required to be supplied. One Canadian criminologist charged with contempt for failing to disclose confidential information relating to the identities of research participants (Palys and Lowman 2000) won his case on the basis that the information had been obtained in confidence, confidentiality was essential to the research relationship, that the research was socially valuable, and that the harm of breaching confidentiality outweighed the benefit to be gained by disclosure – the Wigmore test (Nelson and Hedrick 1983; Traynor 1996; and see Lowman and Palys 2001; Lindgren 2002). However, there is no reported Australian case law supporting a clear 'researcher privilege' and even in North America there are significant questions over its

---

14 *Gartside v Outram* (1856) 26 LJ Ch 113; *Initial Services v Putterill* (1968) 1 QB 396.

15 *Lion Labs v Evans* (1984) 2 All ER 417; X v Y (1987) 13 IPR 202.

16 Some statutory protection for whistleblowers confers immunity for 'appropriate' disclosures of public interest information by public officials, subject to many qualifications.

existence and breadth, with recent decisions more commonly rejecting a specific privilege but taking confidentiality issues into account along with other factors.[17]

As researchers, we need to be aware of the implications of the formal agreements we make. We have a stark choice – comply or risk the consequences of contravention. Such agreements may displace most of the common law and equitable rules relating to confidentiality (though not all agreements do so and some explicitly preserve such general obligations). However, researchers and research participants cannot rely on the provisions of a confidentiality agreement between the discloser and recipient to avoid making disclosures that are legally compelled or block those that are legally permissible under the public interest defences.

In short, researchers who receive information under such agreements need to ensure that those agreements contain adequate general categories of exemption and that they do not inadvertently restrict researchers from using or disclosing information that they would otherwise have a legitimate entitlement to use such as information in the public domain or already known to the researcher.

Epidemiological Studies (Confidentiality) Acts

In Australia, some researchers may receive statutory protection for their data. Various acts, including the Epidemiological Studies (Confidentiality) Act 1981 (Commonwealth) and the Epidemiological Studies (Confidentiality) Act 1992 (Australian Capital Territory), impose a statutory duty to maintain confidentiality of any information concerning the affairs of another person where that information was gathered as part of a 'prescribed study' (Cica 1994; Bronitt 1995).

While few criminologists regard themselves as epidemiologists, this legislation is relevant to criminology because of the breadth of the definition given to the term 'epidemiological study'. In the Commonwealth legislation this includes research into the 'the incidence or distribution' of an 'activity, form of behaviour, course of conduct, or state of affairs, that is or may be disadvantageous to, or result in a disadvantage to, the person concerned or to the community' (s.3(1)).

---

[17] See eg *Burka v U.S. Dep't of Health & Human Servs.*, 87 F.3d 508, 515 (D.C. Cir. 1996), and discussion in that case of *Anker v G.D. Searle & Co.*, 126 F.R.D. 515, 519 (M.D. N.C. 1989) *In re Snyder,* 115 F.R.D. 211, 213 (D. Ariz. 1987); *Wright v Jeep Corp.*, 547 F. Supp. 871, 876 (E.D. Mich. 1982).

However, researchers have found both the Commonwealth and the Australian Capital Territory legislation to be quite unwieldy as they apply only to large government-backed projects that are officially prescribed. The Australian Capital Territory Act does not appear to allow disclosure of information in the public interest (Cica 1994) and Commonwealth laws can only cover prescribed epidemiological projects conducted by or on behalf of the Commonwealth government (Loxley et al. 1997). By 1988, ten studies had been listed under the Commonwealth Act, seven of which were being conducted by the National Campaign Against Drug Abuse. No studies were listed between 1988 and 2000 and, by 1996, there was an 18-month waiting period for studies to be considered (Fitzgerald and Hamilton 1996). Lorraine Beyer's study of high-level trafficking of heroin is one of the more recent studies to obtain protection under the Commonwealth legislation. Beyer described the difficulties that she faced:

> Primarily through our doggedness and determination was this achievement accomplished. This hugely cumbersome and time-consuming process was the *only* way in which this relatively simple research project was able to proceed. (Beyer 2003: 3)

Similarly, feasibility research on the controlled availability of opioids by the National Centre for Epidemiology and Population Health and the Australian Institute of Criminology was prescribed under the Australian Capital Territory legislation. The heroin project finally started in 1991, three years after the researchers applied for funding. Since then, only four other studies have been prescribed under the Act.

A further reason for scepticism in relation to the value of state or territory based legislation like the Epidemiological Studies (Confidentiality) Act 1992 is that the protection it purports to offer may not be legally effective. In the case of *Chapman v Luminis Pty Ltd* [No 2] [2000] FCA 1010, Von Doussa J held that the prohibition of disclosure of certain information contained in the *Aboriginal Heritage Act 1983* (South Australia) was inconsistent with the Commonwealth Evidence Act, and hence invalid to the extent of that inconsistency (under section 109 of the Constitution).

Privacy Laws

Laws relating to the privacy of personal information may overlap with confidentiality obligations, providing protection for the same subject matter. However, the potential implications of privacy controls for research are less well understood than those relating to confidentiality.

Australia has a complex and inconsistent set of statutory privacy laws and administrative rules, operating at the Commonwealth and State and Territory levels. These include the: Privacy Act 1988 (Commonwealth) and related guidelines issued by the Privacy Commissioner; [18] Privacy and Personal Information Protection Act 1998 (New South Wales); Information Privacy Act 2000 (Victoria); Information Act 2002 (Northern Territory); and the mixture of administrative controls and guidelines largely based on the Information Privacy Principles embodied in the Commonwealth Privacy Act applied in Queensland,[19] South Australia [20] and Tasmania [21] (none of which have significant privacy statutes). There is also a range of special controls on certain types of information, including material relating to health, tax and credit details.

Most of these laws have been developed to govern the use of personal information held by government departments and agencies in their routine processing of government business and transactions with individuals.[22] While the laws do cover personal information held by research bodies, the fit is awkward as the controls are not well designed for research data.

These laws are primarily directed at 'information privacy', protecting information about people, rather than extending privacy rights more generally. They set down basic standards to be applied to the collection, storage, use and disclosure of 'personal information'. Personal information is defined in the Commonwealth Act as 'information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material

---

18 For further information on the Commonwealth privacy laws see http://www.privacy.gov.au.

19 Administrative Information Standards, approved by Cabinet on 10 September 2001.

20 See Information Privacy Principles introduced by means of a Cabinet Administrative Instruction in July 1989.

21 Information Privacy Principles: Guidelines for Agencies, in August 1997.

22 There are special exceptions for certain types of medical research (conducted in accordance with guidelines under s.95 of the Commonwealth Privacy Act 1988), and the Victorian Information Privacy Act 2000 does contain some more general references to and exceptions for some research applications (see further below).

form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion'.

The controls only come into play in relation to information where the individual concerned is identifiable, or can be re-identified either based on reasonable inference or on matching with other retained coded information. So, researchers can avoid becoming subject to the legislation if the information used or stored is anonymous or permanently de-identified and the identity of the person cannot be readily inferred.

In some situations, additional protections apply to certain classes of information that are deemed 'sensitive'. The Victorian Information Privacy Act defines sensitive information as personal 'information or an opinion about an individual's: racial or ethnic origin; political opinions; membership of a political association; or religious beliefs or affiliations; philosophical beliefs; membership of a professional or trade association; membership of a trade union; sexual preferences or practices; or criminal record'. It is not difficult to see how the topics favoured by criminologists might fall into these categories.

Depending on the particular laws and facts, a private organisation[23] may be subject to the same laws or different but similar controls (such as the National Privacy Principles under the Commonwealth Privacy Act).

A public research institution in Australia will usually be subject to those privacy controls that apply to its own jurisdiction. However, where a researcher is working in a different jurisdiction or accessing research data gathered in another jurisdiction, it may also be subject to the controls of that other jurisdiction. There may be tensions between the two sets of controls. The complication of multiple controls may also be triggered by specific contractual provisions in contracts relating to access to relevant data, or even in contracts funding the research. Research that involves the exchange or transfer of information across national borders may raise even more fundamental problems. Researchers may either have to deal with both sets of control or, where the laws are not sufficiently compatible, it is conceivable that such transborder transfers may be blocked.[24]

---

[23] This term includes an individual; a body corporate; a partnership; any other unincorporated association; or a trust – but excludes certain small businesses, political parties, Commonwealth Government agencies and State or Territory authorities and prescribed instrumentalities of a State or Territory.

[24] See discussion below of the Victorian Information Privacy Act 2000, which controls disclosure of data across the Victorian border. See also Principle 9 (Transborder data flows) of the National

The National Statement requires that a Human Research Ethics Committee 'be satisfied that the research proposal conforms with all Commonwealth, State or Territory privacy legislation or codes of practice' (NS 18.1). It indicates that an acceptable standard of protection of personal information is conformity with the Information Privacy Principles of the Privacy Act 1998 (Commonwealth) (NS 18.2). The National Statement also indicates that 'where personal information about research participants or a collectivity is collected, stored, accessed, used or disposed of, a researcher must strive to ensure that the privacy and confidentiality of participants and/or the collectivity are respected, and any specific agreements made with the participants or the collectivity are to be fulfilled' (NS 1.19).

The potential implications for researchers that flow from the Commonwealth Information Privacy Principles and the Victorian Information Privacy Act 2000 are considered in more detail in Section Three of this report, but we provide a brief overview here.[25]

Commonwealth Information Privacy Principles

Researchers can access the various principles and related guidelines on-line.[26] In brief, the key principles require:

- proper consent from participants, including making them aware of the research purpose and likely end recipients of the information (IPP2)
- that information be used primarily only for that original purpose (with certain exceptions (IPP10)
- proper storage and security for information (IPP4)
- heavy restrictions on disclosure of personal information (IPP 11)

Other principles cover issues such as: fair and lawful collection of information (IPP 1); collection of relevant and complete information (IPP 3); allowing the data subject to have access to records about their personal information – except if required or permitted by other laws to deny such access (IPP 6); taking reasonable steps to ensure records are kept accurate, relevant, up to date,

---

Privacy Principles (these differ from the Information Privacy Principles, which do not contain such a restriction).

[25] See also the commentary on privacy issues in section 18 of the Human Research Ethics Handbook (National Health and Medical Research Council 2001) http://www.nhmrc.gov.au/hrecbook/01_commentary/18.htm.

[26] See http://www.privacy.gov.au.

complete and not misleading, processing requests by individuals to alter data (IPP 7, 8); and only using personal information for relevant purposes (IPP 9).

The Federal Privacy Commissioner can permit acts that would otherwise breach privacy principles by reaching a public interest determination. The Australian Institute of Criminology was able to make use of this in 1991 in order to allow access to material held by the Australian Federal Police.[27] Further, ethics committees have the power to approve research that infringes the IPPs of the *Privacy Act 1988* (Commonwealth) in specified circumstances. Although this does not appear to apply to social and behavioural research, Human Research Ethics Committees may approve medical and health research that does not conform with the IPPs if the research conforms to either *Guidelines approved under Section 95A of the Privacy Act* applying to information held by Commonwealth agencies or *Guidelines Under Section 95 of the Privacy Act 1988* applying to information held in the private sector (NS at 52-53).

State-based privacy laws

As we have already noted, a wide variety of privacy controls exist across Australia. We discuss some of the implications of the Commonwealth, New South Wales and Victorian controls in Section Three of this report. We do not provide an exhaustive review of these matters and researchers need to be familiar with the controls that exist in the particular jurisdictions in which they gather personal information. For example, the Victorian legislation includes special restrictions on the covert collection of data and on the transfer of data across the Victorian border. There is a special exception in relation to use or disclosure in relation to ASIO and ASIS requests that may be relevant to some types of criminological research (see Principle 2(h)). Unusually, the Victorian Act also provides a limited research exemption (in Principle 2) where use or disclosure of information:

> …is necessary for research, or the compilation or analysis of statistics, in the public interest, other than for publication in a form that identifies any particular individual –
> (i) it is impracticable for the organisation to seek the individual's consent before the use or disclosure; and

[27] See Section Three.

(ii) in the case of disclosure – the organisation reasonably believes that the recipient of the information will not disclose the information.

It is important to remain up to date as many of those controls are likely to change as some jurisdictions implement more rigorous and legislatively-based privacy controls. Apart from materials available on the web,[28] there are several looseleaf services and other materials that discuss privacy compliance in more detail,[29] (though they do not necessarily contain material tailored to the needs of researchers). Researchers should consult their own institutional policies and seek specific advice as required from institutional legal advisers.

Case Law

Recent case law in Australia points to the possible development of a new common law tort of invasion of privacy. Obiter comment by the High Court in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* [2001] HCA 63 explicitly left the door open to the evolution of such a tort in the future. More significantly, a Queensland District Court decision of *Grosse v Purvis* [2003] QDC 151 awarded compensatory damages for 'Breach of Right to Privacy', although that case did relate to sustained 'stalking'. In subsequent decisions, higher courts have held that the law has not developed to the point where an action for breach of privacy is recognised in Australia – see *Giller v Procopets [2004] VSC 113*, *Kalaba v Commonwealth of Australia* [2004] FCA 763 and *Kalaba v Commonwealth of Australia* [2004] FCAFC 326.

However, if such laws did develop, they would extend beyond simple information privacy, providing a broader based right to privacy. This is unlikely to have any significant impact on the conduct of consensual research (provided that researchers protect the storage and use of personal information), but such case law may conceivably have an impact on some observational research where consent is not obtained.

Freedom of Information Legislation and Archive Requirements

By and large, Freedom of Information laws are unlikely to require researchers to provide access to sensitive research data. Research material generally falls

[28] See http://www.privacy.gov.au and links.

[29] See CCH Privacy Law & Policy Reporter; LexisNexis Privacy Law Bulletins.

under exemptions that exist for researchers and for private or confidential data, though the extent of the exemption varies between jurisdictions.[30]

However, some archive requirements oblige researchers to retain some of their records, reinforcing the need for researchers to consider carefully both what documents they need to create in the first place, and how much identifying information needs to be included in them. Requirements may be statute based,[31] or flow from institutional policies. For example, s.24 of the Commonwealth Archives Act 1983 (which applies to Commonwealth and Australian Capital Territory agencies, including the Australian National University) controls the disposal and destruction of Commonwealth records, but does enable destruction in accordance with the individual administrative policies of agencies.[32]

Laws compelling disclosure of information

Australian researchers are not immune from general laws authorising warrants or subpoenas or other forms of compulsory disclosure of information exercised by law enforcement bodies or under court backed sanction, despite the obvious ethical dilemmas involved. In this section, we provide a brief introduction to the general laws relating to subpoenas and admissibility in the research context, and consider the additional powers that various agencies may have to compel disclosure of information. Subpoenas are considered first, prior to discussion of general rules on admissibility of evidence and privilege, as the question of compliance with subpoenas preceeds any question of the admissibility of evidence.[33]

Subpoenas, admissibility of evidence and privilege

Subpoenas are a common tool available to participants in litigation to ensure access to that information required to run their case. As subpoenas are potentially very powerful, they are subject to checks and balances and courts retain discretion as to whether or how they are enforced. It is possible to apply to

---

30 See the Human Research Ethics Handbook: a Research Law Collection http://www.nhmrc.gov.au/hrecbook/pdf/hrechand.pdf at L31 (National Health and Medical Research Council 2001).

31 For example, Archives Act 1983 (Commonwealth); Public Records Act 2002 (Queensland); State Records Act 1997 (South Australia).

32 See, for example, the Australian National University policies (Responsible Practice of Research: available at http://info.anu.edu.au/policies/Policies/Research/Other/Responsible_Research_Practice.asp. The data storage and retention and confidentiality elements largely mirror the Joint NHMRC/AVCC Statement and Guidelines on Research Practice.

33 See *Northern Territory of Australia v GPAO* [1999] HCA 8 Gleeson CJ and Gummow J [16, 72]

have subpoenas set aside by the court or to vary their application. Subpoenas may be set aside if they are an abuse of process, oppressive (because they constitute an undue burden, are unreasonable or too vague), or lack relevance. However, there is no general 'researcher privilege', and an applicant who relied on the negative impact on privacy or confidentiality will not usually be able to avoid a subpoena, although such issues may influence the way in which the subpoena is applied.

Failure to comply with a subpoena is a serious matter, as it could place a researcher in contempt of court (see, for example, the Federal Court Rules – Order 27 Rule 12). Any researcher receiving a subpoena must treat it seriously and should seek legal advice whether a court might set it aside or vary its application. Even if the subpoena cannot be set aside, there may be significant grounds for confining its application to specific forensic purposes, or persuading the court to impose special limitations on access to or use of the information, or even redacting relevant data. Such factors would be considered on a case by case basis.

There is little relevant case law in Australia to indicate what impact subpoenas could have on researchers. The nearest case law relates to research conducted in support of (or in contemplation of) litigation. However, the example of *Clarrie Smith v Western Australia* [2000] FCA 526 is useful to consider. In that case, an expert anthropologist had taken notes about Aboriginal beliefs in the course of preparing a report in relation to Aboriginal Heritage Act claims. The applicant sought to avoid releasing the information arguing that the confidential material had been supplied to the researcher 'on the basis of his professional undertakings'. In that case, Madgwick J referred to the well-known test for public interest privilege stated by Gibbs ACJ in *Sankey v Whitlam* (1978) 142 CLR 1 at 38, and observed that confidentiality was not 'in itself considered to be sufficient to ground a claim for public interest immunity (although it may be relevant to the exercise of the Court's discretion whether to permit access to the materials)'. The judge permitted the subpoena to stand but reconciled the competing interests by restricting access to the documents and requiring certain gender sensitivities to be observed. Similar restrictions were applied in the context of the Hindmarsh Island Bridge litigation: see *Chapman v Luminis Pty Ltd* [No 2] [2000] FCA 1010. Orders were made pursuant to ss 17(4) and 50 of the Federal Court of Australia Act 1976 (Commonwealth) that 'evidence about the restricted women's knowledge be adduced in camera in the presence of only one female legal practitioner representing each group of parties in the

proceedings, and that the evidence received not be disseminated without further order of the Court'.

Of course, apart from the initial issue of compliance with subpoenas, general rules on admissibility of evidence and privilege need to be considered. With the exception of the statutory protection provided by the Epidemiological Studies (Confidentiality) Acts, there are no specific privileges that a researcher can rely on that relate to the research status of their activities or records. However, the court does have a general discretion to exclude evidence.[34] So, a judge may refuse to admit evidence if its probative value is substantially outweighed by the danger that the evidence might be unfairly prejudicial to a party, be misleading or confusing, or cause or result in undue waste of time. The court could take into account the fact that evidence included confidential communications, but there is no blanket or automatic protection. Even if evidence is not excluded, the courts also have a general discretion to limit use of that evidence.

Other possible sources of compelled seizure or disclosure

There are numerous other ways in which research data might conceivably be subject to some form of compulsory seizure, including police warrants, so-called Anton Pillar orders, and other statutory mechanisms that give certain agencies (especially law enforcement agencies) special powers. Police warrants usually require the authorisation of a senior police officer and any seized evidence may be submitted to a court. Anton Pillar orders are civil search and seizure orders by which any aggrieved party with a serious complaint can obtain from a court (in the absence of the other party) an order compelling access to property and the ability to seize evidence which may be destroyed. Apart from the police, a wide range of organisations have special powers to seize information or even compel responses. These include anti-corruption commissions such as the New South Wales Police Integrity Commission, Royal Commissions and State, Territory and Federal parliaments. A brief summary of some of the more notable agencies with such powers follows in Table One, with links to further information:

Australian Crime Commission	http://www.crimecommission.gov.au/
Australian Security Intelligence Organisation	http://www.asio.gov.au/
Australian Secret Intelligence Service	http://www.asis.gov.au/

[34] see eg Evidence Act 1995 (Commonwealth) s.135

Australian Securities and Investments Commission	http://www.asic.gov.au/
Police Integrity Commission (NSW)	http://www.pic.nsw.gov.au/
Independent Commission Against Corruption (NSW)	http://www.icac.nsw.gov.au/
Crime and Misconduct Commission (Qld)	http://www.cmc.qld.gov.au/
Corruption and Crime Commission of WA	http://www.ccc.wa.gov.au/

Table One: Some of the Australian organisations with special powers to seize information or compel disclosure of confidential information.

Carrington and the Police Integrity Commission

In 1999, Kerry Carrington was summonsed to appear before the New South Wales Police Integrity Commission to discuss aspects of the police investigation into the Leigh Leigh murder case. Unusually, Byrne-Armstrong et al. (1999) published an article discussing what they described as 'an unpleasant encounter between legal culture and feminist criminology':

When Kerry Carrington was summonsed to appear before the PIC inquiry she was provided with virtually no information about the purpose and scope of the inquiry as it related to her. What she was told turned out to be misleading. She was cross-examined for three days by six counsel... the only purpose served by most of this cross examination was to afford counsel for the police (and the PIC) the opportunity to attack Kerry Carrington's credibility in respect of matters the PIC had no intention of investigating... Fragments from radio interviews, some that occurred almost four years before, were quoted (or sometimes misquoted) and explanations sought for this particular phrase or that sentence, no opportunity being afforded (if possible) for her to read the whole transcript or to recollect the circumstances of the interview. (pp.23-4)

There are also special investigative powers that may be available to a number of agencies under specific statutes. Any of these may affect criminological researchers, particularly those receiving data via electronic modes of communication. For example, the power to intercept communications under the Telecommunications (Interception) Act 1979 (Commonwealth), and the recent amendments introduced by the Telecommunications (Interception) Amendment

(Stored Communications) Act 2004 (Commonwealth), provide expanded powers to intercept stored email, SMS and voice mail (especially unread material). It is difficult to predict what impact the new powers will have. Indeed, while there are general reporting obligations in relation to the use of these powers, the detail of this use may not be publicly reported.

Since many of these powers may have a draconian effect, they are usually accompanied by a set of checks and balances in their execution, and there will be later opportunities for appeal or judicial review. A researcher may not be able to resist the initial execution of such warrants or powers, but may be able to subsequently argue about appropriate access to or use of the information, and raise privacy and confidentiality considerations. Even if such arguments do not result in a complete removal of the threat, courts may modify the end effect of the orders and reduce the impact on pre-existing obligations of confidentiality and privacy. Of course, researchers should seek legal advice immediately if they find themselves subject to the exercise of such powers.

In short, researchers are not above the law and there is no general privilege or ground under Australian law on which researchers can rely to have their research excluded from evidence. The potential for compulsory disclosure of information under court order is something that researchers should bear in mind throughout the research process, from design to publication.

Section Three: Frequently Asked Questions

Many of the difficulties that researchers confront in caring for their data are shared across the social sciences. Yet, in many cases, researchers feel like they are the first to confront their particular problem. Based on a review of the social science literature and the experience of lawyers who work in this area, we have identified a series of frequently asked questions about how researchers may gather, store, use, disclose and reuse information. We have clustered our responses into three broad categories (see Table Two) that review the procedures that researchers are required to adopt in gathering information, the ways that researchers can and cannot use data, and the pressures that researchers may face from or through the legal system to disclose data. Using case studies, we also provide guidance on how to respond to the difficulties and manage the risks involved.

What procedures do researchers need to follow?

1. *What factors should researchers take into account in designing a study?*
2. *How should researchers negotiate access to data?*
3. *What data and methods contravene the law?*
4. *What do researchers owe the people who provide them with data?*

How are researchers supposed to store their data?

5. *Do I have to keep records? For how long?*
6. *How should I store and secure records?*
7. *Do I need to de-identify data?*

How can and can't researchers use their data?

8. *Can I use information gathered for one purpose for another purpose?*
9. *If research is done under contract, can that impact on how I can use the information I gather?*
10. *Are there restrictions on publication of data?*
11. *Are there restrictions on sharing data with other researchers?*
12. *How do privacy controls impact on disclosure of information to others?*
13. *Can I transfer personal data across state or national boundaries?*
14. *Are there restrictions on re-using data for other purposes?*

How can the law be used to pressure researchers to disclose information?

15. *How are researchers vulnerable to subpoenas, police warrants and other forms of legally compelled disclosure?*
16. *Can researchers be compelled to disclose information under research-related contracts?*
17. *How should I respond to possible contractual obligations to disclose information?*
18. *How should I respond to mandatory notification requirements?*

Table Two: List of Frequently Asked Questions addressed in this section.

Q1 – What factors should researchers take into account in designing a study?

Primarily, will the research design (type of information sought, methods for obtaining, manipulating and storing data) have a negative impact on participants? We need to consider the potential obligations we may come under to disclose information (including under subpoena or contract). Given this, are there ways of legitimately designing an appropriate study that minimise risks, perhaps by enabling participants to contribute information anonymously or by otherwise limiting or removing the need to record sensitive identified data in the first place? If data can be provided anonymously, or if it is otherwise possible to design studies so as to avoid recording identified personal information, then researchers will usually avoid privacy law complications. Indeed some Federal

and Victorian privacy principles explicitly encourage researchers to provide options for anonymous participation.[35]

Carefully consider relevant confidentiality issues at the research design stage, including the possible future reuse of datasets or disclosure of datasets to others. Ensure that these matters conform with consent procedures for participants. Where sensitive information does need to be recorded, can it be safely stored and de-identified?

Q2 – How should researchers negotiate access to data?

When collecting personal identified information, under privacy laws (in addition to ethics requirements) researchers first need to obtain proper consent from participants. It is a fundamental principle in soliciting information to make sure the individual is aware why the information is being collected and to whom it might be passed (Commonwealth IPP 2). This has clear implications for the initial briefing protocols and information sheets prepared for research participants. Collection of information should not intrude to an unreasonable extent upon the personal affairs of the individual (IPP 3). This will not affect information gathered in a consensual fashion, but may have implications for surreptitious collection of data (such studies may raise special ethical issues in any event).

The way researchers obtain consent from participants may also be influenced by the approaches taken by individual research ethics committees. However, written consent is not the only way to obtain consent, and indeed it is not necessarily evidence of truly informed consent. Various commentators have observed that signed informed consent forms can be impractical and may decrease response rates or skew responses, and that voluntariness can be assured by other briefing practices (Roberts and Indermaur 2003; Israel 2004b). Consider other approaches such as verbal or implied consent, or active interrogation of a potential participant's understanding of the study by the researcher. Indeed, it is possible that procedures other than written consent forms may actually improve the quality of the consent, especially if there is some active questioning of understanding by the researcher once an initial briefing has been provided (in written or other form) to the potential participant. In

[35] Victorian Privacy Principle 8.1 provides that '[w]herever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organization'. This is clearly directed more at situations of government service provision, and it is subject to a broad cut out of practicability. At a Federal level consider also National Privacy Principle 8 - which requires options for anonymity wherever practicable and lawful, along with other guidelines from the Federal Privacy Commissioner generally encouraging anonymity as an option, available at http://www.privacy.gov.au.

contrast, a signature on a form does not guarantee any real level of understanding, nor even that the person executing the document has read it.

When designing consent procedures and information sheets (or other briefing protocols) for participants, consider whether these are consistent both with the immediate research needs and other potential future research needs. Consider methodologies for altering sensitive data to protect participant interests, by de-identification or other means.

Human Research Ethics Committees and Informed Consent

Some researchers have argued that their ability to respect confidentiality has been compromised by the way that some HRECs have interpreted informed consent. The National Statement requires researchers to obtain the informed and voluntary consent of participants except in specific, defined circumstances (NS 1.7). Researchers are generally expected to record participants' agreement to take part. Often this will involve asking participants to sign a form. The National Statement allows consent to be established using 'other sufficient means' (NS 1.9) but this option is not explored in much detail in the National Statement and some HRECs have proved unwilling to sanction alternatives to formal written declarations of consent. In some cases, researchers interpreted HRECs' insistence on signed forms as evidence of legal risk management rather than a desire to protect research participants (Roberts and Indermaur 2003). In other cases, criminologists believed that the requirement that they obtain signed forms would jeopardise the research, compromising assurances of anonymity and confidentiality (and thus creating a conflict with the fundamental obligation recognised by the National Statement to protect participants), reducing the response rate, or affecting the validity of the study.

Among other things, researchers should ensure that participants have substantial understanding of the research, risks and potential benefits. According to the Human Research Ethics Handbook, this might mean that participants should be advised of 'the means of protecting confidentiality' or 'if there is a possibility of confessions of illegal activity or reportable conduct, whether researchers may be mandated to disclose this to the relevant authorities' (L17)

A person who is not given sufficient information and agrees to a procedure to which he or she would not have agreed if adequately informed, may be able to sue

in negligence if he or she suffers injury or loss as a result of the procedure, even if there is no negligence in its actual performance (Human Research Ethics Handbook L15).

Q3 – What data and methods contravene the law?

There are few direct restrictions on data and methods, provided that these do not breach other laws (such as stalking laws) and receive ethical clearance. However, tension is created when the opportunities presented by the availability of data and the possibilities for its analysis must be weighed against the need to respect the privacy of citizens about whom the data is recorded. While researchers may emphasise the need to ensure the flow of information, inevitably the methodologies of some research projects will need to be compromised to protect personal information, while other projects will simply not be able to be conducted. So, criminologists have reported that privacy legislation has stopped proposed research in both the Australian Capital Territory and New South Wales (Israel 2004b).

However, the right to privacy that Human Research Ethics Committees are required to uphold is not absolute. In appropriate circumstances a committee should consider the risk and magnitude of harm from what must often be technical breaches, and weigh that against the equally valid rights of others, and against matters that benefit society as a whole.

Some researchers working with agencies that operate under Federal jurisdiction have been able to take advantage of provisions in the Commonwealth Privacy Act (1988). Unlike some state legislation, the Commonwealth Privacy Act allows the Federal Privacy Commissioner to determine where the balance might lie in a particular research project. In the case of social research, applications must be made by an agency.[36]

[36] See http://www.privacy.gov.au/act/publicinterest/index.html

Federal Privacy Commissioner

On two occasions, the Federal Privacy Commissioner has allowed personal information held by government agencies to be disclosed to the Australian Institute of Criminology for the purposes of research. In 1991, the Australian Federal Police were allowed to disclose personal information relating to homicides in the Australian Capital Territory to enable research to be carried out under the national homicide monitoring program (Public Interest Determination No. 5).[37] Although the Federal Privacy Commissioner did consider asking the police to cull or de-identify files, the Commissioner concluded that it would 'tend to defeat the objects of the research' (p.4) and accepted that criminological research was 'an activity which can at least at times involve collecting data in a personally-identified form' (p.3). The Institute's Director was reported as giving evidence that 'it was commonplace in criminological research for researchers to be given access to complete files and that important studies in relation to the causes of crime in such areas as sexual offences would have been impeded without access to personal particulars in the initial stages of the research' (p.5).

Again, in 2002, the Commonwealth Director of Public Prosecutions was authorised to disclose 28 Commonwealth files containing personal information relating to serious fraud to enable research to be carried out by Russell Smith (Public Interest Determination No. 8).[38] The files contained psychiatric assessments of offenders, the names of accused persons, witnesses and police informants whose safety could be threatened by public disclosure. While the police in other jurisdictions had been willing to accept personal undertakings from the researchers that they would not record or disclose the identities of individuals or organisations named in the documents (Smith 2003), such a decision was not open to Commonwealth agencies because of the 1988 Act. Again, the Commissioner considered asking the Director of Public Prosecutions to cull or de-identify files, but the Commissioner concluded that it would 'be unreasonably resource intensive and would likely impede the objects of the research' (p.8). He also accepted that there was no other way that the research could be conducted and that it would be impracticable to gain the consent of those people who might be affected by the decision.

[37] http://www.privacy.gov.au/publications/pid5.html

[38] http://www.privacy.gov.au/publications/pid8.html

In each case, the information to be disclosed, the means of disclosure, the use to which the information would be put, the person to which the information would be disclosed were all restricted, and the need for all published data to be anonymised was imposed (Smith 2003). In the second case, the Commissioner placed a further restriction on the publication of the research – it had to be published 'in such a way as to prevent the information being used to inspire or facilitate the commission of crime' (p.3). At the end of the process, Russell Smith (2003: 10) concluded that:

Even with the cooperation of willing agencies, the expenditure of considerable resources, and plenty of time, carrying out research of this nature is not for the faint-hearted. (p.10)

In Victoria, the Privacy Commissioner cannot authorise a breach of the Information Privacy Principles (IPPs). However, the Privacy Commissioner (Chadwick 2003) has pointed out that agencies can register a code of practice covering particular types of research or certain data sets as a substitute for the IPPs. In addition, guidelines could be developed to ensure that the IPPs are consistently interpreted in commonly recurring research contexts.

One area of heated ethical debate among social scientists is the degree to which deliberate manipulation or concealment of information – involving covert observation, deception by lying, withholding information or misleading exaggeration – might be warranted in research. The First Consultation Draft (National Health and Medical Research Council et al. 2004) recognises the value of deception, concealment or covert observation in exceptional circumstances (s2.2). This excludes the kind of undercover research that has been advocated by some social scientists (Bulmer 1982). Researchers who wish to engage in deceptive or covert practices need to be aware that such activities would fall foul of privacy laws if researchers recorded personal information that allowed individuals to be identified (due to the lack of consent and the operation of principles such as Victorian Information Privacy Principle 10 (Sensitive Information)). So, covert observation may be acceptable, but undercover exposé-style reporting of named corporate officers would not be.

Q4 – What do researchers owe the people who provide them with data?

At an ethical level, researchers owe people that are research participants a duty to avoid causing them harm. We also owe them obligations to protect the confidentiality and privacy of information that they provide to us. However these obligations may not be absolute obligations, as there are some legal exceptions

and defences (though there would be complex ethical issues to be considered by a researcher contemplating disclosure in breach of a prior undertaking of confidentiality). Researchers are also not legally immune to various forms of compelled disclosure (see later). As a result, when we are discussing issues of confidentiality and privacy with participants, it is advisable not to overstate our ability to ensure these protections, or misrepresent relevant laws or contractual undertakings. We ought not give unqualified promises of confidentiality and privacy if we are not willing and able to follow through in practice (and risk possible contravention of laws or subpoenas in the process). Clearly conflicts may arise between ethical obligations to protect participants and legal obligations to disclose documents or information (see Q15-18). We provide general advice for responding to subpoenas (Q15), and that includes further consideration of the interests of confidential sources and study participants.

Q5 – Do I have to keep records? For how long?

Maintaining records is usually a part of good research practice. However, in some situations it may be sensible to design research to avoid the necessity to create certain records in the first place (hence reducing the risks of potential confidentiality and privacy complications), or at least to avoid the creation of records with identifiable personal information (Q1, 3). If records have been created then researchers need to be aware of the possible application of Archives legislation or institutional policies on archiving data. It is sensible to take steps to de-identify personal and identified information once it is no longer needed in that form, and the Privacy Commissioner recommends this procedure as a security measure.[39] However, it can be quite difficult (especially in a networked environment) to erase all copies of digital data, and researchers should understand that information may still be backed up in other locations or accessible even if they delete a working or archived copy.

Q6 – How should I store and secure records?

Once information is gathered, it must be properly stored and secured (IPP 4). Researchers must protect records by securing against loss, unauthorised access, use, modification or disclosure, or any other misuse. Given the nature of the data collected in criminological research, this may require special measures beyond those generally applied in a researcher's institution.[40] Depending on the exact circumstances, these safeguards may need to be as high as that for

---

[39] Federal Privacy Commissioner's Information Sheet 9 – 2001 Handling Health Information for Research and Management available at http://www.privacy.gov.au/publications/IS9_01.html.

[40] See the Federal Privacy Commissioner's Information Sheet 6 – 2001 Security and Personal Information http://www.privacy.gov.au/publications/IS6_01.html

sensitive health data,[41] – including special access restrictions on information systems, encryption, 'stand-alone'[42] data storage and processing, and physical security for hardcopy records – and should be continually reviewed in the light of technological developments.

The Joint NHMRC/AVCC Statement and Guidelines on Research Practice (National Health and Medical Research Council 1997) provides that research institutions should have clearly formulated policies on issues including the maintenance of records, retention of data, management of intellectual property and confidentiality (1.3). While the statement does not have the force of law and is currently being reformulated as the Australian Code (National Health and Medical Research Council et al. 2004), observation of its requirements may be a condition of institutional policies or contract provisions, and in any event it provides a reasonable standard for general reference. More particularly the statement details further requirements relating to data storage and retention in item 2. Data are meant to be recorded in a durable and appropriately referenced form and managed consistently with relevant privacy protocols and standards. These standards will obviously shift over time and the detail of relevant standards will change with (while lagging behind) technological developments in data storage and use. This places a fairly high burden on researchers dealing with personal information to ensure that the degree of protection given to such information remains sufficient to cope with what will probably be increasingly strict demands to protect personal privacy. Individual departments or research units need data retention and storage procedures as much original data should be stored at the unit level in case there is a need to respond to allegations of data falsification. Data are meant to be held for sufficient time to allow reference (examples between five to 15 years are given). Researchers are responsible for ensuring appropriate security for any confidential material, including that held in computing systems, and the statement stresses the need to pay particular attention if data is stored on networks.

---

41 See HB 174-2003: Information security management – Implementation guide for the health sector which is based on and interprets AS/NZS ISO/IEC 17799:2001-Information Technology-Code of Practice for Information Security. Note that AS4400-1995 'Personal privacy protection in health care information systems', a standard referred to in many privacy information sheets, appears now to have been withdrawn by Standards Australia from publication.

42 Remote from (and not connected to) usual data networks used for general academic purposes.

Q7 – Do I need to de-identify data?

In Victoria, in addition to the types of general controls discussed under the Commonwealth principles, there is a further requirement on data security – (Principle 4.2): 'An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose.' While subject to a fairly broad exemption that would permit retention for reference and archive purposes as well as further permitted research purposes, this does put an ongoing obligation on affected researchers to review retained data and destroy or de-identify it if no longer required.

Q8 – Can I use information gathered for one purpose for another purpose?

If a record that contains personal information was obtained for a particular purpose then under privacy laws it cannot be used for any other purpose (IPP 10) unless the individual concerned has consented to such use or the use falls under certain exceptions. Those exceptions include: where the record-keeper reasonably believes that such use is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person; such use is required or authorised by or under law; such use is reasonably necessary for enforcement of the criminal law or of a law imposing a financial penalty, or the purpose for which the information is used is directly related to the purpose for which the information was obtained.

This control may have a significant impact on the re-use of information originally gathered for another purpose. Additional use may require further consent from the relevant individuals, unless the new purpose can be seen to be 'directly related to the purpose for which the information was obtained'. While from an ethical perspective a research ethics committee can approve data being used for later (possibly not directly related) research purposes, a commitee has no authority to absolve breaches of statutorily based privacy principles.

Q9 – If research is done under contract, can that impact on how I can use the information I gather?

If work has been done under contract then consider what impact that contract might have through, for example, additional privacy and confidentiality controls, obligations to record/disclose data, and intellectual property issues. Researchers should try to amend any contract terms and conditions that might be inconsistent with their research design or implementation prior to execution. After the contract is signed, researchers should remember the relevant contract terms and not simply 'file and forget' those obligations. Pass information about key provisions onto others involved in conducting the research.

Q10 – Are there restrictions on publication of data?

Obviously, publication of confidential or private information must be avoided unless consent is obtained. De-identified data summaries and resultant conclusions and discussion may not pose any publication problems in relation to such issues, unless there is a risk of re-identification, by foreseeable data matching, inference or otherwise.

Q11 – Are there restrictions on sharing data with other researchers?

Consider whether the original terms of acquisition of the information permit this. Is it consistent with past undertakings of confidentiality, privacy, or limitations on the purpose for which the data was acquired? Again, thinking ahead at the outset to the possibility or necessity for such data sharing and clearing it with participants can head off later problems. If data is provided to other researchers, then (depending on sensitivity and relevant laws and undertakings) it may need to be provided under conditions that control the nature and extent of use, and compel the recipient to observe relevant privacy and confidentiality laws and undertakings. This may require a formal confidentiality agreement.

Q12 – How do privacy controls impact on disclosure of information to others?

IPP 11 heavily restricts disclosure of personal information and may prevent disclosure of information to third parties for research purposes. This can have several consequences. Researchers may be unable to obtain information from otherwise willing providers, or may be unable to engage in multi-centre or derivative research projects. Researchers are not permitted to disclose personal information to others unless: the participant is reasonably likely to have been aware that information of that kind is usually passed on to such recipients; the participant has consented to the disclosure; or the other exceptions already discussed in relation to IPP 10 apply.

A person to whom personal information is disclosed under IPP 11 must not use or disclose the information for a purpose other than the purpose for which the information was given.

Record keepers may also be subject to administrative obligations that require them to maintain publicly accessible records about the general nature of personal information they keep (IPP 5). The type of records that must be maintained include: the nature of the records of personal information kept; the purpose for which each type of record is kept; the classes of individuals about whom records are kept; the period for which each type of record is kept; the

persons who are entitled to have access to personal information and the conditions under which they are entitled to have that access; and the steps that should be taken by persons wishing to obtain access. These must be made available for inspection by members of the public and a copy must be given to the Privacy Commissioner annually. In a sensitive research context such as criminology, full compliance with these controls will be difficult and may be undesirable from a broader privacy perspective. However, in relation to consensual research, it seems unlikely that compliance failures would trigger complaints from the participants involved.

Q13 – Can I transfer personal data across state or national boundaries?

Victorian Privacy Principle 9 (Transborder Data Flows) provides that data can only be transferred between jurisdictions if: there is a reasonable belief that the recipient is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the (Victorian) Information Privacy Principles (whether the Commonwealth principles would be sufficiently similar is not clear); or with consent from the individual and the disclosing organisation has taken reasonable steps to ensure that the information will not be held, used or disclosed by the recipient inconsistently with the (Victorian) Information Privacy Principles.

Similar privacy restrictions may complicate transborder data flows across country borders. This is certainly an issue in relation to personal information sent out of Europe, and out of a number of other jurisdictions throughout the world that have followed a European approach.

Q14 – Are there restrictions on re-using data for other purposes?

Again, consider whether this is permissible, given the limitations of the original data acquisition, the briefings given to participants, and relevant privacy laws such as those discussed above. If intentions for reuse are considered up front, then researchers might avoid having to acquire additional consent from participants (see Q8).

Q15 – How are researchers vulnerable to subpoenas, police warrants and other forms of legally compelled disclosure?

Several criminologists in the United States and Canada have been served with warrants and subpoenas, often marking the start of a stressful and unpleasant process for them. There is no general 'researcher privilege', and an applicant who relied on the negative impact on privacy or confidentiality will not usually

be able to avoid a subpoena, although such issues may influence the way in which the subpoena is applied, or the information is used.

The best time to think about the impact of a subpoena might be at the research design stage. If a researcher can sensibly avoid the creation of documents with sensitive identified information in the first place, then clearly such problems can be avoided. Michael Traynor (1996) identified a range of techniques that researchers can use both while planning and conducting their research as well as after legal action is initiated. While Traynor's recommendations related to the American legal system, many of his suggestions should be relevant to Australian jurisdictions.

The planning stages	Identify reasons for confidentiality
	Give confidentiality assurances sparingly
	Obtain statutory confidentiality protection, if available
Research in progress	Unlink names and identifying details of sources from confidential data and safeguard the data
	Comply with requirements of your institutional research ethics committe
After the subpoena arrives	Consult with your management and legal counsel immediately
	Notify confidential sources and study participants when there is risk of disclosure
	Make timely service of written objections
	Negotiate an acceptable limitation of subpoena or move to quash or modify it
	Seek an adequate protective order
When disclosure has been ordered	Seek recovery for costs of compliance with subpoena when possible and appropriate
	Request a court order that may help protect you from liability for disclosure and/or require party who issued subpoena to indemnify you
	If trial court orders disclosure of confidential data, consider requesting a stay as well as review by an appellate court
	Develop constitutional issues and policy questions and preserve significant matters for appellate review
	Consider refusing to obey a final and binding court order of disclosure and going to jail for contempt

Table Three: Strategies for Countering Subpoenas for Research (adapted from Traynor 1996)

Researchers have acted to protect the confidentiality of research participants and their activities by either not seeking or recording names and other data at all, or by removing names and identifying details of sources from confidential data at the earliest possible stage. These precautions offer the advantage of

helping to guard data against theft or improper disclosure by other members of a research team.

Methodological responses

During his qualitative research with property criminals in the United States, Ken Tunnell took a range of methodological precautions. He:

...never spoke participants' names during the recorded interviews, which were themselves quickly transcribed and the tapes erased. Although I kept an identifier list and assigned numbers to pertinent information obtained from individuals' case files, names were not connected to the information from the files or interviews. (1998: 208)

Working with street children in Haiti, Kovats-Bernat, an American anthropologist, was concerned that his notes would be used by the state's Anti-Gang Unit to arrest the children. Avoiding detailed field notes, at times he relied on a combination of 'meticulous memorization of entire conversations' and surreptitiously scribbled jottings on 'scraps of paper that I kept in my boot' (2002: 216). He urged other researchers working in dangerous places to remind themselves daily that 'some of the things that we jot down can mean harassment, imprisonment, exile, torture, or death for our informants or for ourselves and take our notes accordingly.' (Kovats-Bernat 2002: 216; see also Salovesh 2003, on his work as an anthropologist in Mexico).

Several researchers have counselled research participants not to give them specific information such as names or details of past criminal events for which they had not been arrested (Hall and Osborn 1994; Sluka 1995; Decker and van Winkle 1996; Feenan 2002) or future crimes that they planned to commit (Cromwell *et al.* 1991). Other researchers have reported sending files out of the jurisdiction, and avoiding using the mail or telephone system so that data could not be intercepted or seized by police or intelligence agencies (Sluka 1989, 1995; Decker and van Winkle 1996; Feenan 2002; Kovats-Bernat 2002).

One way that researchers have responded to demands by third parties during court cases to see their research data has been to offer redacted material, that is information where the identity of study participants has been removed. In some cases, such as those involving short questionnaires, redacting data may be quite easy. In other cases, it may place an enormous burden on researchers. For

example, in *Deitchman v. E.R. Squibb and Sons*[43] in 1984, the manufacturer of the drug diethylstilbestrol (DES) sought all the information contained in the University of Chicago's DES Registry of 500 cases. The Registry refused to breach patient confidentiality and Squibb offered to accept the data stripped of identifying information. The task was described by the Chairman of the Department of Obstetrics and Gynecology at the University as 'herculean' (Crabb 1996; Wiggins and McKenna 1996).

Q16 – Can researchers be compelled to disclose information under research related contracts?

Contractual obligations may compel disclosure in several ways. First, any funding contract relating to the research may contain specific obligations in relation to matters such as confidentiality, privacy, intellectual property rights, disclosure and publication. Many of these may be reasonable requirements for the funding agency to seek and may simply act in support of the common law and statutory obligations of confidentiality and privacy. To this extent such contracts may not pose a problem. However some obligations may, intentionally or otherwise, not be compatible with the intended research methodology and the interests of participants or other data providers. Contractual obligations may also impact on researchers when researchers obtain information under contract from a third party. This party might be a direct research participant (under a confidentiality agreement or as a consequence of part of a consent agreement), or another researcher or organisation.

In their review of confidentiality issues arising as a result of sharing administrative data gathered as part of American welfare programs, Brady and his colleagues (2001) provided a range of examples that they thought should be specified in any written contract (see Table Four).

[43] 740 F.2d 556 (7th Cir. 1984).

- Prohibition on redisclosure or rerelease
- Specification of electronic data transmission (e.g. encryption methods for network access)
- Description of storage and/or handling of paper copies of confidential data
- Description of storage and/or handling of electronic media such as tapes or cartridges
- Description of network security
- Requirement for notification of security incidents
- Description of methods of statistical disclosure limitation
- Description of disposition of data upon termination of contract
- Penalties for breaches

Table Four: Contractual Procedures for Protecting the Confidentiality of Individuals in Research Projects using Administrative Microdata Files (from Brady *et al.* 2001: 255)

Q17 – How should I respond to possible contractual obligations to disclose information?

Proposed contracts should be carefully drafted and evaluated from the beginning and adjusted by negotiation to ensure they are compatible with other obligations and the research methodology. For instance, it may be important to restrict the obligations to provide data and results to the funding agencies to avoid an obligation to provide all raw data. Consider for example the absolute audit powers available to the Australian Research Council under clause 29 of the conditions for 2005 Linkage Grants.[44] These allow the Australian Research Council to access to all material. Similarly, any material generated under the terms of a Criminology Research Council Grant Contract must be provided to the Criminology Research Council (see clause 10, and breadth of definition of Contract Material in clause 1). It may also be necessary to ensure the contract fits with other pre-existing or likely contractual obligations. For example, the blanket access rights referred to in relation to the 2005 Linkage Grants are subject to 'any agreement to the contrary with an Industry Partner which can be justified to the satisfaction of the ARC on the grounds of commercial sensitivity (including Intellectual Property considerations)' (see clause 29.2(a)). Therefore if

[44] http://www.arc.gov.au/rtf/LP2005_Funding_Agreement_Website_16Dec04.rtf

the blanket access provisions in these terms were potentially problematic, the matter might be addressed via agreement between the Industry Partner and the Australian Research Council, or by amending the grant agreement between the Institution and the Australian Research Council.

We would hope that any sensible argument to protect reasonable confidentiality and privacy interests of participants or data providers to enable research will be supported by the organisation funding that research. However any variation to a 'standard form' research contract will usually pose delays and difficulties in negotiation. It can be helpful to craft any necessary changes in as simple a form as possible, and to clearly state the purpose and context of these amendments, as often the lawyers or contract administrators involved in drafting, reviewing and amending such contracts lack that information and so may be ill-equipped to deal with such requests.

Q18 – How should I respond to mandatory notification requirements?

All Australian jurisdictions have mandatory reporting requirements, requiring particular professionals to report to community services departments a specific range of activities involving child abuse or neglect. Unlike the United States, these provisions do not extend to elder abuse (Kinnear and Graycar 1999). The National Health and Medical Research Council's (2001) Human Research Ethics Handbook advises that Human Research Ethics Committees ensure that researchers have taken account of the fact that they might uncover information about illegal conduct in the design of their research, have contemplated what their actions will be, and that they are aware of any legal obligations they may be under to report relevant information.

The range of professionals and organisations required to report varies widely between jurisdictions ranging from only a few highly specific professional groups working directly for the court or child care agencies in Western Australia to anyone who has reason to believe that a child may be abused or neglected in the Northern Territory (Australian Institute of Health and Welfare 2005). There is some evidence that some professional groups are either wrong about or uncertain what their obligations are under such legislation (Goddard et al. 2002).

In New South Wales, it is an offence under s 316 *Crimes Act 1900* not to report information about commission of a 'serious offence'. However, in the case of information obtained by a 'researcher for professional or academic purposes', a

prosecution can only be launched for this offence with the approval of the Attorney General. This makes it less likely that a researcher will be charged. Other legislative prescriptions about reporting offending behaviour are rare.

While no jurisdiction specifically lists researchers or academics as a professional group that is subject to mandatory notification legislation, people engaged in research may find that they are subject to reporting requirements because of their other professional roles. Where researchers who are subject to reporting requirements in another capacity believe that there is a possibility that they will find out about child abuse, they may need to consider ways of distinguishing between their different kinds of work. Obviously, this can be particularly difficult for professionals who engage in action research.

So, researchers in South Australia who are also psychologists, police or probation officers, social workers or teachers or are employees of, or volunteers, in government departments, agencies or local government or non-government agencies that provide health, welfare, education, childcare or residential services wholly or partly for children may need to make certain either that research participants understand the role in which the researcher is acting or that the researcher is subject to mandatory reporting provisions. A similar list exists in Tasmania.

In the United States, researchers who wished to explore child abuse but who were concerned that they might be subject to mandatory notification used masking methodologies that ensured that information about child abuse was not linked to the informant (Socolar et al., 1995). For example, in quantitative research on child abuse and neglect, a North Carolina research team (Kotch 2000) required participants to seal their responses to sensitive questions. These responses were then separated from other information that might have identified the respondent. Such deliberate engineering of a methodology to avoid the reporting requirements was not without its critics.

Section Four: Likely future developments

Over the last 20 years, there have been considerable changes in the laws that govern and impact upon criminological research in Australia. However, the changes have not been uniform or consistent, and have varied in impact across both sphere of law and jurisdiction.

The most significant changes have been in the area of privacy, although the various Commonwealth and state laws, regulations and guidelines are both inconsistent and difficult to interpret in the context of criminological research. It is likely that the evolution of privacy laws and codes will continue. Note that there is currently a review into the operation of the private sector provisions of the Privacy Act.[45] One of the terms of reference of the enquiry is that it attempt to '[recognise] important human rights and social interests that compete with privacy, including the general desirability of a free flow of information'. In a number of the submissions to the enquiry there have been calls from researchers and ethics committees for simplification and standardisation of privacy controls and concern at their current negative impact on the ability to undertake research. While advocating change, researchers will need to develop and maintain awareness of and ensure compliance with these laws. This will be particularly complex where research involves the transfer of data across state or national boundaries. Further change may also be driven by Australia's need to bring its privacy laws into harmony with those of its international trading partners, in particular the European Union.[46]

On the other hand, it seems unlikely that there will be dramatic change in the ways confidentiality laws impact on criminological researchers. However, there may be an increased emphasis on contractual confidentiality issues, especially in the context of research funded under contract by an agency, or research that requires access under contract to confidential data held by an agency.

This should not prevent criminological researchers lobbying for improved recognition of the particular context within which we operate, and the difficulties we can face in relation to issues of confidentiality and privacy. The problems in this area are obvious, and we have already discussed them:

---

45 http://www.privacy.gov.au/act/review/index.html

46 Europe has still not formally recognised Australia's data protection laws as being 'adequate' and providing equivalent protection to European Directive 95/46/EC. As a result, information flows from EU countries to Australia may be restricted. See http://europe.eu.int/comm/internal_market/privacy/adequacy_en.htm

> …in these days of litigation and complex privacy and ethical requirements I don't think it is reasonable – never mind good policy – to continue to compromise researchers and the participants in research. I think it is timely for researchers to join together to lobby for change and for legislative protection… Without it researchers will continue to place themselves and their research participants at risk and policy and practise will continue to be based on restricted research that may be biased. (Beyer 2003)

The Western Australian Law Reform Commission (2002) has also repeatedly called for reform to codify and strengthen the discretion that courts have to excuse witnesses from disclosing information in breach of a confidential relationship in judicial proceedings.

In North America, there have been moves to codify and strengthen researcher privileges. For instance, in the United States, the Thomas Jefferson Researcher's Privilege Act of 1999[47] sought to protect researchers from compelled disclosure of research in Federal courts, and would have provided protection from Freedom of Information requests as well as including a specific privilege for research information, covering:

> unpublished lecture notes, unpublished research notes, data, processes, results, or other confidential information from research which is in any progress, unpublished or not yet verified, and any other information related to research, the disclosure of which could affect the conduct or outcome of the research, [or] the likelihood of similar research in the future…

Short term legislative change to protect the confidentiality of criminological research data seems unlikely. In the absence of such reform, desirable as it may be, researchers will need to continue to approach these matters on a case by case basis. Some problematic issues may be able to be avoided by appropriate research design. However, researchers will need to be vigilant to protect the confidentiality and privacy of research data (at all stages of gathering, manipulation, use and disclosure), and meet both general legal and institutional governance requirements. They should also consider the possibility that their

[47] Introduced July 26, 1999 106th Congress 1st Session S. 1437, http://thomas.loc.gov/cgi-bin/query/z?c106:S.1437.IS. Current status: Referred to Senate committee, read twice and referred to the Committee on Judiciary.

data will have to be disclosed under various legal provisions, and be prepared to argue on a case by case basis for adequate protection.

It is tempting to view legal matters in isolation, but clearly the way that legal issues affect criminologists will be partly mediated by the ethical governance of criminological research. In other work, we identified the difficulties that the National Health and Medical Research Council and the various Human Research Ethics Committees have had in clarifying the relationship between law and ethics (Israel 2004b). Criminologists have found their research blocked or modified beyond recognition in the past. Despite current revision of both the National Statement and the Australian Code for Conducting Research, we believe that fear of legal risk will continue to drive this process. We hope that this report will help criminologists and their institutions reach better informed decisions about legal risks.

Bibliography

Allen, A.L. (1997) Genetic Privacy: Emerging Concepts and Values, in M.A. Rothstein, ed., *Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic Era*. New Haven, CT: Yale University Press. pp. 31-59.

American Sociological Association (1997) *Code of Ethics*. http://www.asanet.org/members/ecoderev.html

Australian Institute of Health and Welfare (AIHW) (2005) Child protection Australia 2003–04. AIHW cat. no. CWS 24. Canberra: AIHW (Child Welfare Series no. 36). http://www.aihw.gov.au/publications/cws/cpa03-04/cpa03-04.pdf

Beauchamp, T.L. and Childress, J.F. (2001) *Principles of Biomedical Ethics* (5th ed.). New York: Oxford University Press.

Beyer, L. (2003) The role of ethics in research. Paper presented at the *Evaluation in Crime and Justice: Trends and Methods Conference*, Canberra, 24-25 March.

Bok, S. (1983) *Secrets: The Ethics of Concealment and Revelation*. New York: Random House.

Brady, H.E., Grand, S.A., Powell, M.A. and Schink, W. (2001) Access and Confidentiality Issues with Administrative Data. In Ver Ploeg, M., Moffitt, R.A. and Citro, C.F. (eds) *Studies of Welfare Populations: Data Collection and Research Issues*. Washington DC: National Academy of Sciences, pp.220-74.

Brajuha, M. and Hallowell, L. (1986) Legal Intrusion and the Politics of Fieldwork: The Impact of the Brajuha Case. *Urban Life* 14, pp.454-78.

Bronitt, S. (1995) Criminal Liability Issues Associated with a 'Heroin Trial'. Feasability Research into the Controlled Availability of Opioids Stage 2, *Working Paper 13*. National Centre for Epidemiology and Population Health. Canberra: the Australian National University. http://nceph.anu.edu.au/Publications/Opioids/work13a.pdf

Bulmer, M. (ed.), (1982) *Social Research Ethics: An Examination of the Merits of Covert Participant Observation*. New York: Holmes and Meier.

Byrne-Armstrong, H., Carmody, M., Hodge, B., Hogg, R. and Lee, M. (1999) The risk of naming violence: an unpleasant encounter between legal culture and feminist criminology. *Australian Feminist Law Journal* 13, pp.13-37.

Carroll, J. and Knerr, C. (1973) Confidentiality of Social Science Research Sources and Data: the Popkin Case. *Political Science Quarterly* 6, pp.268-80.

Chadwick, P. (2003) *Social Research and Privacy*. Address to the Managing Diversity Forum. 21 May. http://www.privacy.vic.gov.au/dir100/priweb.nsf/download/E1949B4389C395D5CA256D3500819A54/$FILE/OPE_privacy_21503.pdf

Cica, N. (1994) Civil Liability Issues Associated with a 'Heroin Trial'. Feasability Research into the Controlled Availability of Opioids Stage 2, *Working Paper 11*. National Centre for Epidemiology and Population Health. Canberra: the Australian National University. http://nceph.anu.edu.au/Publications/Opioids/work11a.pdf

Crabb, B.B. (1996) Judicially Compelled Disclosure of Researchers' Data: A Judge's View. *Law and Contemporary Problems* 59/3, pp.9-34. http://www.law.duke.edu/journals/lcp/index.htm

Cromwell, P.F., Olson, J.N. and Wester Avary, D'A. (1991) *Breaking and Entering: an Ethnographic Analysis of Burglary*. London: Sage.

Decker, S.H. and Van Winkle, B. (1996) *Life in the Gang: Family, Friends and Violence*. Cambridge: Cambridge University Press.

Dickson, D. (1999) Complaint Upheld against University Ethics Committee. *Nature America* 5/11, p.1224.

Farrar, S. (1999a) Suicide Row Hits Aids Research. *Times Higher Education Supplement,* 10 September.

Farrar, S. (1999b) Researcher in Aids Suicide Case wins Exeter Ethics Dispute. *Times Higher Education Supplement*, 24 September.

Feenan, D. (2002) Legal Issues in Acquiring Information about Illegal Behaviour Through Criminological Research. *British Journal of Criminology* 42, pp.762-81.

Fitzgerald, J. and Hamilton, M. (1996) The Consequences of knowing: Ethical and Legal Liabilities in Illicit Drug Research. *Social Science and Medicine* 43/11, pp.1591-600.

Fitzgerald, J.L. and Hamilton, M. (1997) Confidentiality, Diseeminated Regulation and Ethico-Legal Liabilities in Research with Hidden Population of Illicit Drug Users. *Addiction* 92/9, pp.1099-107.

Gillett, G. (1987) AIDS and Confidentiality. *Journal of Applied Philosophy* 4/1, pp.15-20.

Gillis, A.M. (1992) The Unwilling Expert: Lawyers Discuss Confidentiality Issues, Compelled Disclosure of Scientific Data, and Scholars' Testimony. *BioScience* 42/3, pp.160-3.

Goddard, C.R., Saunders, B., Stanley, J. and Tucci, J. (2002) *A Study in Confusion – Factors which affect the decisions of community professionals when reporting child abuse and neglect*. Australian Childhood Foundation and the National Research Centre for the Prevention of Child Abuse at Monash University, Melbourne.
http://www.aaca.com.au/downloads/A_Study_in_Confusion.pdf

Hall, K.J. and Osborn, C.A. (1994) The Conduct of Ethically Sensitive Research: Sex Offenders as Participants. *Criminal Justice and Behavior* 21, pp.325-40.

Israel, M. (2004a) Strictly Confidential? Integrity and the Disclosure of Criminological and Socio-Legal Research. *British Journal of Criminology* 44/5, pp.715-40.

Israel, M. (2004b) *Ethics and the Governance of Criminological Research in Australia*. Sydney: Bureau of Crime Statistics and Research.
http://www.lawlink.nsw.gov.au/bocsar1.nsf/files/r55.pdf/$file/r55.pdf

James, J. (1972) 'On the Block': Urban Research Perspectives. *Urban Anthropology*, 1/2, pp.125-40.

Kershaw, D. and Fair, J. (1976) *The New Jersey Negative Income-Maintenance Experiment. Volume 1: Operations, Surveys and Administration*. New York: Academic Press.

Kinnear, P. and Graycar, A. (1999) Abuse of older people: crime or family dynamics? *Trends and Issues* 113 .
http://www.aic.gov.au/publications/tandi/ti113.pdf

Kotch, J.B. (2000) Ethical Issues in Longitudinal Child Maltreatment Research, *Journal of Interpersonal Violence* 15/7, pp.696-709.

Kovats-Bernat, J.C. (2002) Negotiating Dangerous Fields: Pragmatic Strategies for Fieldwork amid Violence and Terror. *American Anthropologist* 104/1, pp.208-22.

Lindgren, J. [2002] Discussion: Anticipating Problems-Doing Social Science Research in the Shadow of the Law *Sociological Methodology* 32:29-32

Lowman, J. and Palys, T. (2000) Ethics and Institutional Conflict of Interest: the Research Confidentiality Controversy at Simon Fraser University. *Sociological Practice: a Journal of Clinical and Applied Sociology* 2/4, pp.245-64.

Lowman, J. and Palys, T. (2001) The Ethics and Law of Confidentiality in Criminal Justice Research: A Comparison of Canada and the United States. *International Criminal Justice Review* 11, pp.1-33.

Loxley, W., Hawks, D. and Bevan, J. (1997) Protecting the Interests of Participants in Research into Illicit Drug Use: Two Case Studies. *Addiction* 92/9, pp.1081-5.

Maisel, L.S. and Stone, W.J. (1998) The Politics of Government-funded Research: Notes from the Experience of the Candidate Emergence Study. *PS: Political Science and Politics* 31/4, pp.811-17.

McCollum, K. (1999) Appeals Court Cites Researchers' Rights in Denying Microsoft's Request for Notes, *Chronicle of Higher Education*. 8 January, p.A31.

McKeough, J. and Stewart, A. (2002) *Intellectual property in Australia* (3rd ed.). Sydney: Butterworths.

McLaughlin, R.H. (1999) From the Field to the Courthouse: Should Social Science Research be Privileged? *Law and Social Inquiry* 24/4, pp.927-65.

McNabb, S. (1995) Social Research and Litigation: Good Intentions Versus Good Ethics. *Human Organization* 54, pp.331-4.

National Health and Medical Research Council (1997) *Joint NHMRC/AVCC Statement and Guidelines on Research Practice*.
http://www.nhmrc.gov.au/research/general/nhmrcavc.htm

National Health and Medical Research Council (1999) *National Statement on ethical conduct in research involving humans*.
http://www.health.gov.au:80/nhmrc/publications/synopses/e35syn.htm

National Health and Medical Research Council (2001) *Human Research Ethics Handbook: Commentary on the National Statement on Ethical Conduct in Research Involving Humans*.
http://www.nhmrc.gov.au/hrecbook/pdf/hrechand.pdf

National Health and Medical Research Council, Australian Research Council and Australian Vice-Chancellors' Committee (2004) *Draft Australian Code for Conducting Research*. http://www.nhmrc.gov.au/research/general/code.htm

Nelson, R.L. and Hedrick, T.E. (1983) The Statutory Protection of Confidential Research Data: Synthesis and Evaluation. In Boruch, R.F. and Cecil, J.S. (eds) Solutions to Ethical and Legal Problems in Social Research. New York: Academic Press.

Norris, C. (1993) Some Ethical Considerations on Field-Work with the Police. In Hobbs, D. and May, T. (eds) *Interpreting the Field: Accounts of Ethnography*. Oxford: Clarendon Press, pp.123-43.

O'Neil, R.M. (1996) A Researcher's Privilege: Does any Hope Remain? *Law and Contemporary Problems* 59/3, pp.35-50.
http://www.law.duke.edu/journals/lcp/index.htm

Palys, T. and Lowman, J. (2000) Ethical and Legal Strategies for Protecting Confidential Research Information. *Canadian Journal of Law and Society* 15/1, pp.39-80.

Palys, T. and Lowman, J. (2002) Anticipating Law: Research Methods, Ethics, and the Law of Privilege. *Sociological Methodology* 32/1, pp.1-17.

Palys, T. and Lowman, J. (2003) *An Open Letter dated 28 January, to: Marc Renaud, President, Social Sciences and Humanities Research Council, Tom Brzustowski, President, National Science and Engineering Research Council, Alan Bernstein, President, Canadian Institutes for Health Research.*

Picou, J.S. (1996) Compelled Disclosure of Scholarly Research: Some Comments on High Stakes Litigation. *Law and Contemporary Problems* 59/3, pp.149-58. http://www.law.duke.edu/journals/lcp/index.htm

Roberts, L. and Indermaur, D. (2003) Signed consent forms in Criminological Research: Protection for Researchers and Ethics Committees but a threat to research participants? Paper presented at the *Evaluation in Crime and Justice: Trends and Methods Conference*, Canberra, 24-25 March.

Salovesh, M. (2003), Contribution to On-line *Chronicle of Higher Education* Colloquy 10 May http://chronicle.com/colloquy/2003/notes/

Scarce, R. (1999) Good Faith, Bad Ethics: When Scholars go the Distance and Scholarly Associations do not. *Law and Social Inquiry* 24/4, pp.977-86.

Shaw, J. (2002) Privacy – How to Make Your Business Compliant. Lexis Nexis.

Sluka, J.A. (1989) *Hearts and Minds, Water and Fish: Support for the IRA and IINLA in a Northern Irish Ghetto*. Greenwich, CT: JAI Press.

Sluka, J.A. (1995) Reflections on Managing Danger in Fieldwork: Dangerous Anthropology in Belfast. In Nordstrom, C. and Robben, A.C.G.M. (eds) *Fieldwork under Fire: Contemporary Studies of Violence and Survival*. London: University of California Press. pp.276-94.

Smith, R. (2003) *Methodological Impediments to Researching Serious Fraud in Australia and New Zealand*. Paper presented at the *Evaluation in Crime and Justice: Trends and Methods Conference*. Canberra, 24-25 March. http://www.aic.gov.au/conferences/evaluation/smith.html

Socolar, R.R.S., Runyan, D.K. and Amaya-Jackson, L. (1995) Methodological and Ethical Issues Related to Studying Child Maltreatment. *Journal of Family Issues* 16/5, pp.565-86.

Traynor, M. (1996) Countering the Excessive Subpoena for Scholarly Research. *Law and Contemporary Problems* 59/3, pp.119-48. http://www.law.duke.edu/journals/lcp/index.htm

Tunnell, K.D. (1998) Honesty, Secrecy, and Deception in the Sociology of Crime: Confessions and Reflections from the Backstage. In Ferrell, J. and Hamm, M. (eds.) *Ethnography at the edge: crime, deviance, and field research*. Boston: Northeastern University Press. pp.206-20.

Van Maanen, J. (1983) The Moral Fix: On the Ethics of Fieldwork. In Emerson, R.M. (ed.) *Contemporary field research: a collection of readings*. Boston: Little, Brown. pp. 269-87.

Western Australian Law Reform Commission (2002) 30th Anniversary Reform Implementation Report: Law Reform Commission of Western Australia, 1972-2002. Perth: The Commission.

Wiggins, E.C. and McKenna, J.A. (1996) Researcher's Reactions to Compelled Disclosure of Scientific Information. *Law and Contemporary Problems* 59/3, pp.67-94. http://www.law.duke.edu/journals/lcp/index.htm

Wilson, R. (2003) Penn Anthropologist Fights Subpoenas for Field Notes in Medical Case. *Chronicle of Higher Education* 49/28. 21 March, p.A14.

Wolfgang, M.E. (1982) Confidentiality in Criminological Research and Other Ethical Issues. *Journal of Criminal Law and Criminology* 72/1, pp.345-61.

List of Statutes

Commonwealth

Archives Act 1983

http://www.comlaw.gov.au/comlaw/legislation/actcompilation1.nsf/current/bytitle/3CD836FBEE3B46F9CA256F71004E6DA5?OpenDocument&mostrecent=1

Epidemiological Studies (Confidentiality) Act 1981

http://www.comlaw.gov.au/comlaw/legislation/actcompilation1.nsf/current/bytitle/F07A5766A89487C1CA256F71004DB529?OpenDocument&mostrecent=1

Evidence Act 1995

http://www.comlaw.gov.au/comlaw/legislation/actcompilation1.nsf/current/bytitle/3281AF59F7EE28E5CA256F7100511A2A?OpenDocument&mostrecent=1

Federal Court of Australia Act 1976

http://www.comlaw.gov.au/comlaw/legislation/actcompilation1.nsf/current/bytitle/2B1571ED1BD8CA31CA256F81000FCAFA?OpenDocument&mostrecent=1

Privacy Act 1988

http://www.comlaw.gov.au/comlaw/legislation/actcompilation1.nsf/current/bytitle/9EBFDA7BE1132D11CA256F71004C809E?OpenDocument&mostrecent=1

Telecommunications (Interception) Act 1979 [including specifically amendments introduced by the Telecommunications (Interception) Amendment (Stored Communications) Act 2004]

http://www.comlaw.gov.au/comlaw/legislation/actcompilation1.nsf/current/bytitle/0B14824B1125A44CCA256F860015FF1B?OpenDocument&mostrecent=1

Australian Capital Territory

Epidemiological Studies (Confidentiality) Act 1992

http://www.austlii.edu.au/au/legis/act/consol_act/esa1992382/

New South Wales

Crimes Act 1900

http://www.austlii.edu.au/au/legis/nsw/consol_act/ca190082/

Privacy and Personal Information Protection Act 1998

http://www.austlii.edu.au/au/legis/nsw/consol_act/papipa1998464/

Northern Territory

Information Act 2002

http://notes.nt.gov.au/dcm/legislat/legislat.nsf/d989974724db65b1482561cf0017cbd2/306b17e5e75d2ff069256e99001ba1fb?OpenDocument

Queensland

Public Records Act 2002

http://www.austlii.edu.au/au/legis/qld/consol_act/pra2002153/

South Australia

State Records Act 1997

http://www.austlii.edu.au/au/legis/sa/consol_act/sra1997156/

Victoria
Information Privacy Act 2000
http://www.austlii.edu.au/au/legis/vic/consol_act/ipa2000231/