COPS, COMPUTERS, AND THE RIGHT TO PRIVACY IN THE INFORMATION AGE: UNAUTHORISED ACCESS AND INAPPROPRIATE DISCLOSURE OF INFORMATION COMPLAINTS IN NEW SOUTH WALES

[1]Mike and [2]Lily Enders

[1]School of Policing Studies,
Charles Sturt University,
[2]New South Wales Ombudsman's,
Sydney
New South Wales
menders@csu.edu.au

Keywords
police, computer, access, privacy, information, technology, email, ethics

INTRODUCTION

The term the 'information age' is particularly applicable to Australia. In a recent email, the Australian Institute of Criminology's Chief Librarian, John Myrtle, passed on statistics which showed that internet use and access in Australia has increased about 50% during the last year (Pers. Comm. 14 July 1999). Of greater interest is the fact that almost 20% of Australian households, 1.3 million, have internet access and over one third of the adult population has accessed the internet at some time during the year ending February 1999. To further back these figures, the *Sydney Morning Herald* of 12 February, 2000, carried statistics from the Australian Bureau of Statistics which showed that 22.6% of Australian families had home internet access (Anon., 2000a, p. 105). These figures firmly place Australians among the world's most computer literate societies.
Of course computers weren't always that popular. The authors of this paper entered law enforcement at a time when computers were owned by Universities and major corporations - not individuals - and a decent calculator cost about a week's wages. However, things changed quickly and by the 1980s computers were an established part of policing. Today, all major police services are committed to, and reliant on, some form of computerised information system. The two systems which the authors have had contact with are the Crime Reporting and Information System for Police (CRISP) (Queensland Police Service) and the Computerised Operational Policing System (COPS) (New South Wales Police Service). While many aspects of these two systems are different, they, and all the other police information systems in existence, share one major similarity: they store and provide access to personal and confidential information on every individual with whom police come into contact during their duties. Modern police investigation techniques rely on officers being able to access this information routinely to carry out their duties and fight crime. Likewise, the individuals whose personal information is held on law enforcement computer systems are entitled to a reasonable expectation of privacy. This presents the single greatest dilemma to law enforcement officers using computers: when does investigation and intelligence gathering become common curiosity and therefore unlawful?

IS THERE A PROBLEM?

As early as 1979 it was acknowledged by the New South Wales Police Service (NSWPS) that computer terminals could be manipulated to produce false records such as traffic and fingerprint records. It was also identified that security measures concerning the provisions of documents for court, e.g. a person's criminal record, were inadequate. As recently as 1988, there was a complaint that an officer was paid $1500 to ensure that when a particular person with prior convictions for drink driving appeared in court, their previous record was not mentioned so that they would be treated as a first offender (NSW Ombudsman, 1988).
Unlawfully accessing computer information is an offence in NSW under S309 (1) of the Crimes Act 1900 No. 40 (NSW) (see **Annexure** 1). The offence is complete upon access to data being gained regardless of the intention of the person who accesses the data. If the data is accessed with some intent or if the data is of a specifically confidential nature, a circumstance of aggravation applies and the penalty increases markedly from 50 to 500 penalty units and six months to two years imprisonment.
The Ombudsman's Annual Reports reveal that unlawfully accessing computer information is a major issue in the NSWPS. As **Annexure 2** shows, complaints to the NSW Ombudsman have increased at a fairly consistent rate over the last few years. It could be argued that the more familiar officers have become with computers, the more prevalent unlawful access and related complaints have become. It could also be argued that the number of these complaints is small, an average of 350 each year, compared to the number of employees, about 16,000. Several things need to be considered in this context:

- assuming that each person was only complained about on one occasion, about 15% of employees have been the subject of complaints over the last seven years;
- at worst the complaint trend is increasing, at best it is not decreasing (Brammer claims that the NSWPS figures for 1995-99 represent a downward trend, however, apart from a reduction in the 98-99 year, the figures appear to be stable or increasing (Brammer, 2000, pp. 10-11). The 98-99 results are encouraging.);
- in the 1997-98 year, 99 complaints of inappropriate disclosure were fully investigated, 42% of these investigated complaints resulted in an adverse finding or were conciliated (NSW Ombudsman, 1998, p. 61);
- in the 1997-98 year, 127 access complaints were fully investigated, 57% of these complaints resulted in an adverse finding or were conciliated (NSW Ombudsman, 1998, p. 61);
- there is no guarantee that the figures reflect more than a small proportion of the problem since most access complaints come from **random** checks conducted by the Service; and
- a complaint can involve an enormous number of potential offences (In one case, an officer was found to have committed 1,592 accesses, which even after the impact of statute barring, translated to 71 criminal charges and one departmental charge.).

It is fairly clear that information technology is creating a problem within law enforcement (Brammer, 2000; NSW Ombudsman, 2000). (The recent hearings conducted by the Qld Criminal Justice Commission suggest that the problem is not restricted to NSW.)

These complaint figures are particularly disturbing when one considers that after the introduction of COPS and following the release of an Independent Commission Against Corruption (ICAC) Report on unauthorised release of Government information (ICAC, 1992), the NSWPS instituted a training program for officers to eradicate instances of unlawful access. In fact in the year following the commencement of training, complaints rose from 173 in 93/94 (NSW Ombudsman, 1994) to 217 in 94/95 (NSW Ombudsman, 1995a). The seriousness of these issues led to two reports from the Ombudsman. *Improper access to and use of confidential information by police* (NSW Ombudsman, 1994b) was followed by a further report to Parliament in 1995, *Confidential information and police* (NSW Ombudsman, 1995b). This report set out the 'positive police action' taken by the Service to deal with the problem. The Service's initiatives included a *Statement of responsibility* (see Annexure 3) for information and information systems. Officers were required to sign this *Statement* after completing the training referred to earlier. While not really amounting to a code of ethics for information access, the *Statement* was based on ethical principles and the legal constraints which apply to computer access. Unfortunately, it did not work.

IS THE PUBLIC ENTITLED TO AN EXPECTATION OF PRIVACY

A recent Canadian case, *R v Weir* (1996) involving child pornography provides an excellent example of the degree of privacy the law ascribes to information on a computer network (Geddie, 1999). AB was sent an email message from another person. The message contained an extremely large graphic/video file which contained pornographic images of young children. The file was so large that it jammed the Internet Service Provider to which AB subscribed. While fixing the problem, a technician discovered the content of the file and the police were contacted. The file was copied and given to the police and then delivered to AB's email box. The police obtained a warrant using the copied file and searched AB's home where they found the original file and seized his computer's contents and a disk. AB was charged with possessing child pornography.

The court found that the act of copying the file for the police did not amount to an unwarranted search. More importantly, the Court examined the nature of email compared to regular mail and decided that email carried with it a reasonable expectation of privacy. Therefore, a warrant is required to seize email stored on a computer network. By extension this case confirms that the owner or intended recipient of even a seemingly innocuous email message stored on a computer is entitled to a reasonable expectation of privacy with regard to the data. A recent NSW case involving two women who were awarded $150,000.00 compensation after being sacked over sending emails to each other which defamed a supervisor seems to confirm this finding (Harris, 2000a). Most of the information held on police computer systems is much more confidential in nature than the average email and therefore a higher level of privacy should be expected. Recent privacy legislation passed in NSW should clarify the situation here. Further, in NSW, the provisions of Section 309 (and Section 310) of the *Crimes Act* apply to all computer systems, not just police or government computers. This effectively makes 'computer hacking' in any form an offence.

WHAT HARM IS DONE BY ACCESS?

The nature of computer access offences investigated varies from officers accessing information about themselves through to accessing information to pass on to a third party for payment - corruption. It is obvious from this broad spectrum of breaches that an ethical solution needs to cover a lot of territory. It might be useful at this point to consider a number of case studies to provide a better understanding of what unlawful access means. The cases selected are representative of the types of information access complaints overviewed by the NSW Ombudsman.

Case 1 - Curiosity **(Ombudsman, 1995b, pp. 6-7)**
A random audit of COPS revealed that an officer had accessed COPS on 1591 separate occasions to check on personal details of family, friends, former school class-mates (for a reunion), workmates and various motor vehicles in which he was interested.
The police investigation was not completed until after six months had passed. Eventually the officer was charged with 71 offences under Section 309(3) and one departmental charge of Misconduct. (At this time a statute of limitations of six months existed for offences under S309 (1). It is now two years.)

Case 2 - Noble cause curiosity **(Ombudsman, 1995b, pp. 11-12)**
A member of the public complained that his former brother-in-law, a police officer, had accessed his criminal history. The police officer claimed that he had information connecting the complainant with an armed hold-up.
The explanation provided was found to be flawed in several respects. Further, the officer also breached a Commissioner's Instruction that police officers not involve themselves in matters concerning friends or relatives. There was a clear conflict of interest in this case which was not recognised by the officer. Remarkably, this also went unnoticed by the Service's investigating officer and the Acting Region Commander. The Service found that the complaint was 'unsustained'. The Ombudsman disagreed.

Case 3 - Amnesia and the 'good Samaritan' gone wrong **(Ombudsman, 1995b, pp. 12-15)**
A woman complained that a man had harassed her on two occasions demanding compensation for damage to his motor vehicle. A check of the COPS indicated that a particular officer had accessed the woman's details and might have passed the information to the man whose car was damaged. The officer claimed that he 'could not remember' and that someone else must have used his password or his computer terminal whilst it was unattended.
The officer was attached to the COPS Performance Support Unit and should have taken steps,
in accordance with the Statement of Responsibility to avoid others using his password or active terminal. The matter of officers forgetting to log out of computer terminals received press coverage as recently as July, 1999 (Keogh, 1999) The complaint was sustained.
This particular case is remarkable for the poor quality of advice received by the investigating police from Region Legal Services. The advice seems to exempt police from the provisions of Section 309 by virtue of their office. The Director of Public Prosecutions clarified the matter and established that a charge could indeed be supported in this case.

Case 4 - Corruption **(Ombudsman, 1995b, p. 7)**
As a result of information from ICAC that an officer was passing information to a firm of private inquiry agents, a particular police officer's access of COPS was examined.
The officer was found to have accessed confidential details of a large number of people who were the subject of insurance or small debt claims or family court action. The officer subsequently pleaded guilty to twenty-one charges under Section 309 after being allowed to resign from the Service. He was fined a total of $2,700.

Case 5 - Cyberstalking

There are many cases of male officers accessing the police data base to satisfy their curiosity about people, particularly young women, in whom they have a personal or sexual interest and further indiscreetly disclosing information about those people, e.g. one officer accessed personal details about his dentist's receptionist as he 'liked the look of her' and wanted to find out her age which he then passed on to his male colleagues (NSW Ombudsman, 1992). In another case, a Detective Senior Constable accessed personal information about his ex-wife to ascertain her financial situation and the people she was associating with (NSW Ombudsman, 1993). Another Detective, an Inspector, accessed the criminal history details of his former daughter-in-law's new husband, while another officer charged with assault accessed details of witnesses due to appear in his own court matter (NSW Ombudsman, 1993).

While traditional stalking requires that the activity create fear in the victim, these cases differ in that often the victim is unaware of the stalking until either, the stalker becomes a traditional type of offender, or, often in the case of NSW complaints, an investigator interviews them regarding contact with an officer as the result of internal random audits of information use. The fact that the fear is generated about past events of which they had no knowledge at the time should not diminish the victim's rights to see justice done. There can be little doubt that accessing personal information about individuals constitutes, at worst an attempt or at least preparation for, a stalking type offence. At best it is an unwarranted and unlawful invasion of a person's privacy.

The ease of access to databases afforded by the internet is increasingly putting a strain on people's right to privacy (Harris, 2000b). In the case of police officers, these matters are aggravated by the extent and privileged nature of the information provided to, stored on, and accessible to police officers on the Service computer system (NSW Ombudsman, 2000, pp. 13-15). The Service has a genuine need for information from members of the public and other agencies to investigate crime. The public has a right, supported by legislation to expect that information they give to any agency will be used lawfully. The misuse of computer access by a substantial number of NSW police officers can only reduce public confidence in its police service (Brammer, 2000, p. 3).

Case 6 – Misuse of email and internet access

As stated previously, the NSWPS is experiencing the same problems as other corporations regarding the distribution of offensive material on in-house email networks and the use of the internet to harass others (Harris, 2000a & 2000b; Miranda, 2000). The NSW Ombudsman is currently conducting investigations into this area. One issue which must be a major concern is the amount of time spent by officers gathering and distributing this material, especially in the current climate of claims for more staff and higher salaries (Walsh, 2000).

These cases draw attention to a number of issues which lie at the bottom of computer related complaints:

- curiosity needs to be curbed - at worst curiosity, noble or not, has the potential to do irreparable damage to people's character and reputation;
- police at all levels have great difficulty recognising conflict of interest issues (The NSW Ombudsman has reported to parliament on this specific issue recently.);
- computer related complaints need to be taken very seriously as a corporate issue due to the potential for minor accesses to escalate to corruption;
- the existing training programs and disciplinary system does not seem to be reducing the incidence of breaches;
- officers do not seem to realise the gravity of committing breaches;
- some officers do not seem to receive sufficient supervision regarding time spent using the internet and email; and
- some Police Service senior staff and internal investigators are not aware of relevant legislation or the seriousness with which computer related breaches should be viewed.

RECENT DEVELOPMENTS

Recently other aspects of police misuse of computer technology have received media attention and are being actively investigated - the use of email to transmit sexually explicit material, including pornography, inappropriate jokes and personal comments about staff and clients, and revenge/harassment. (It should be remembered that these issues are not restricted to police officers. It simply shows that the adoption of technology by the NSWPS makes them vulnerable to the same technology-related problems faced by any corporation

(Omond, 2000; Anon., 2000b). It is encouraging to note that the NSWPS is addressing these problems (Brammer, 2000; NSW Ombudsman, 2000).

DOES ETHICS PROVIDE THE ANSWER?

The authors believe that it would be extremely easy to blame a lack of ethics training for problems surfacing due to modern advances in information technology. Ethics is a universal construct and deserves more respect than to be 'trotted' out whenever a problem becomes too hard. If a law enforcement officer does not know the difference between right and wrong before they sit down at a Service computer terminal, giving them a dose of ethics training is not necessarily going to improve the situation. To be effective training should be conducted before officers are faced with the responsibility of accessing any information - including computer data.

The problems emerging with advances in technology are simply blinding policy-makers to the real issue - officers have not been given the training they require. It is easy to train police to use technology. It is much harder to teach them how to use that technology with proper discretion. First they must be taught to respect the trust placed in them when computer access is granted. Trust is a quality which is essential to public office, law enforcement and good governance (Delattre, 1995, pp. 60-61).

If an officer was asked, 'do you have the right to go to a colleague's desk, open their drawer and examine their reports, notes and diaries without permission?' the answer would be a resounding 'no'. Likewise, if they were asked about whether they should pass this information on to another person, the answer would be 'no'. Further, they would not appreciate a colleague searching through their own reports, notes and diaries. This is why locked filing cabinets and paper-based record areas are subject to stringent security. Unfortunately, computer files don't seem to be viewed in the same way. Ultimately, this is all that computer information systems are: the distillation of every police officer's confidential reports, notes and diaries. Only the ease of access has changed. It is possible that this is due to a mindset which views paper as concrete and real and therefore valuable, while electronic data is viewed as abstract and virtual or 'unreal' and therefore worth less.

Some might say that if the information is taken away, the problem will disappear. This is very short-sighted. The information has always been there, it's just that it was difficult to access in the past. Officers need to consider whether their need for information is great enough to justify a phone call to the colleague who wrote the original report before pushing the computer's key. They need to realise that every time they access a computer database they are making a conscious decision which might ultimately be tested by a court of law. This is a point recently reinforced in a *Police Service Notice* (NSWPS, 1999, p. 21).

WHEN IS ACCESS AND DISCLOSURE OK?

Officers should feel free to access computer data whenever they need to in the course of their duties. All that is required is a simple entry in their notebook or existing file explaining the access, the reason and the result. If a police officer is asked by a third party, even another police officer, to access information on their behalf, the officer concerned should consider the matter carefully and either politely refuse or, if sure of the appropriateness, carry out the access and record it along with the result, the name of the person requesting the access and the reason for it. Accesses should never be carried out for a third party if their identity has not been confirmed. If the access relates to a person whom the officer knows, including friends or relatives, there is always a possibility that their involvement could be viewed as a conflict of interest. In this case it is best for them to discuss the matter with a supervisor and request that another officer take over the matter.

Since access offences are complete upon access being achieved, any doubts about an inquiry should be referred to a supervisor before the information is accessed.

SUMMARY

There is little doubt that police services will continue to use technology as it becomes available, including a move to interview people over the internet (Kearney, 2000). It should be remembered that human errors can still occur as Darren Carver can attest (O'Shea, 2000). Darren was falsely charged with two offences after his fingerprints, supplied for elimination when he reported an offence himself, were incorrectly linked to two house breakings. He was only released after successfully convincing police to double-check the fingerprints, something which should, perhaps, have been routine.

Often, one needs to step back and look at the 'big picture' when examining an issue. Computer access and the technology it involves has the capacity to confuse and distort our view of the world when really only the medium for storing and accessing the information has changed. Ethical access to, and use of, information is a constant in an ever changing world. The same issues facing society today were considered when people first learnt to store and spread information, initially using cave walls and rock carvings. The move from an oral tradition to writing and ultimately to the invention of the printing press presented the same concerns to professions about improving

people's access to information that law enforcement agencies face today. One needs to have an increased respect for the right to access information in line with the streamlined access to the information rather than simply restricting the terms of that access. Police work today, particularly intelligence driven policing, requires extensive access to information but the community is still entitled to an assurance that this information will be used in strict accordance with the legislation - after all the community provides most of that information in the first place.

Annexure 1

Offences relating to computers (*Crimes Act 1990 (NSW)*)
309(1) A person who, without authority or lawful excuse, intentionally obtains access to a program or data stored in a computer is liable, on conviction before two justices, to imprisonment for 6 months or to a fine of 50 penalty units, or both.

(2) A person who, with intent
(a) to defraud any person; or
(b) to obtain for himself or herself or another person any financial advantage of any kind; or
(c) to cause loss or injury to any person,
obtains access to a program or data stored in a computer is liable to imprisonment for 2 years, or to a fine of 500 penalty units, or both.

(3) A person who, without authority or lawful excuse, intentionally obtains access to a program or data stored in a computer, being a program or data that the person knows or ought reasonably to know relates to:
(a) confidential government information in relation to security, defence or intergovernmental relations; or...
(c) the enforcement or administration of the criminal law; or...
(e) the personal affairs of any person (whether living or deceased); or...
is liable to imprisonment for 2 years, or to a fine of 500 penalty units, or both.

(4) A person who:
(a) without authority or lawful excuse, has intentionally obtained access to a program or data stored in a computer; and
(b) after examining part of that program or data, knows or ought reasonably to know that the part of the program or data examined relates wholly or partly to any of the matters referred to in subsection 3; and
(c) continues to examine that program or data,
is liable to imprisonment for 2 years, or to a fine of 500 penalty units, or both.

Annexure 2

Computer-related Complaints about Police

Year	Number of Complaints
1992-93	186
1993-94	173
1994-95	217
1995-96	255 (ac)
1996-97	608 (370 ac) (238 id)
1997-98	516 (260 ac) (256 id)
1998-99	495 (264 ac) (231 id)

ac - access complaint
id - inappropriate disclosure of information
(source - NSW Ombudsman's Annual Reports)

Annexure 3
Statement of Responsibility
NSW Police Service
Information and Information Systems

All employees of the NSW Police Service are to abide by the Service's "Code of Best Practice and guidelines for Management of Information and Information Systems" and are accountable to the Commissioner to:
(a) comply with all legal prescriptions regarding the handling of information;
(b) protect information stored in both documentary and computer systems;
(c) treat all information coming to their attention as strictly confidential;
(d) not communicate in any way information regarding police business without proper authority;
(e) report any breaches of security to their Commander or the Commander, Office of Professional Responsibility.
All employees of the NSW Police Service are responsible for the security of information on the Service's computer system. Users must understand and comply with the following protection requirements:
(1) Access [to] computers and computer systems is authorised for the performance of duties only. Information is not to be put to any personal use.
(2) Access to sensitive information is logged. Any users attempting unauthorised access will be called to account by their Commanders and the Assistant Commissioner, Professional Responsibility.
(3) Unauthorised access, including computer games, must not be loaded onto Police Service microcomputer terminals or personal computers.
(4) Passwords must be memorised and kept confidential. Do not display them on or near a terminal. Never disclose passwords even to a supervisor or fellow worker who may seem to have a reasonable request.
(5) Users are required to change their password once a month. Choose a password which is easy to remember but not easily guessed. Passwords must be at least six characters in length.
(6) Users must not leave a logged on terminal unattended. This will prevent another person from accessing information which would in turn be logged against you as a user.
(7) Users will be held accountable for activities which take place under their passwords. If you suspect another person has knowledge of your password you must change it. Report any suspected violations to Commanders.
(8) Appropriate sanctions under the Police Service Act, Public Sector Management Act and Crimes Act shall be applied for misuse and breaches of security.

I have read the Statement of Responsibility and as a user understand my obligations.

Name/Number/Command _____

Signature _____ Date _____

REFERENCES

Anon., (2000a, February 12), Trapped behind the new digital divide, **Sydney Morning Herald**, 101 & 105.
Anon., (2000b, August, 9), Net porn staff caught **The Daily Telegraph**, 9.
Brammer, M. (2000) New South Wales Police Service Response to matters of interest – **CJC Inquiry into Release of Confidential Information**, Sydney: NSWPS Internal Affairs.
Delattre, E. (1995) Keynote Address. In NSWPS (1995) **Ethics/Professional standards seminar** 24, 25 July 1995, NSWPS: Sydney.
Geddie, G. (1999) Email, the police, and the Canadian Charter of Rights and Freedoms: retooling our understanding of a reasonable expectation [of] privacy in the Cyberage. **14th British and Irish Legal Technology Association Annual Conference**, York.
Harris, Sarah (2000a, May 21) Women sacked over e-mails get $150,000 payout, **The Daily Telegraph**, 23.
- (2000b, June 11) Goodbye to privacy, **The Sunday Telegraph**, 113-5.
ICAC (1992) ***Report on unauthorised release of Government information***, ICAC: Sydney.
Jordan, J. (1999) Hierarchies: 0 Networks 1, Management today, June, 10-11.
Kearney, Simon (2000, July 23) Police keen to interview on Internet, **The Daily Telegraph**, 2.
Keogh, Kylie (1999, July 1) Police told to log out, **Daily Telegraph**.
Miranda, Charles (2000, July 26) Police on e-mail alert, *The Daily Telegraph*, 23.
NSW Ombudsman (1988) **NSW Ombudsman 1987-88 Annual Report**, NSW Ombudsman: Sydney.
NSW Ombudsman (1993) **NSW Ombudsman 1992-93 Annual Report**, NSW Ombudsman: Sydney.
NSW Ombudsman (1994a) **NSW Ombudsman 1993-94 Annual Report**, NSW Ombudsman: Sydney.
NSW Ombudsman (1994b) **Improper access to and use of confidential information by police**, NSW Ombudsman: Sydney.
NSW Ombudsman (1995a) **NSW Ombudsman 1994-95 Annual Report**, NSW Ombudsman: Sydney.
NSW Ombudsman (1995b) **Confidential information and police, NSW Ombudsman**: Sydney.
NSW Ombudsman (1996) **NSW Ombudsman 1995-96 Annual Report**, NSW Ombudsman: Sydney.
NSW Ombudsman (1997) **NSW Ombudsman 1996-97 Annual Report,** NSW Ombudsman: Sydney.
NSW Ombudsman (1998) **NSW Ombudsman 1997-98 Annual Report**, NSW Ombudsman: Sydney.
NSW Ombudsman (1999) **NSW Ombudsman 1998-99 Annual Report**, NSW Ombudsman: Sydney.
NSW Ombudsman (2000) **Submission to the Criminal Justice Commission (Qld) on the Misuse of the Queensland Police Service Computer System and the Unauthorised Release of Confidential Police Information**, NSW Ombudsman: Sydney.
NSWPS (1999, June 7) Accessing COPS, **Police Service Weekly**, 11 (22), 21.
Omond, J. (2000) Do not disturb, **Management today**, August, 26-7.
O'Shea, Frances (2000, August 2) The fingerprint that nearly ruined Darren Carver, **The Daily Telegraph**, 9.
Walsh, Philippa (2000, July 18) Cheating the boss, **The Daily Telegraph**, 11.