COPS Database Forum: Recent Cases and Issues

The NSW Council for Civil Liberties in conjunction with the Law Society of New South Wales held a forum on the Computerised Operational Policing System (**COPS**) database. This is a report about the forum, including the topics that were discussed.

Vicky Kuek, the Principal Policy Officer at the Law Society acknowledged the traditional owners and introduced the panel: Jackson Rogers, the NSW Council for Civil Liberties' Convenor – Justice, Police & Mental Health Action Group (Chair); Camilla Pandolfini, Senior Solicitor at the Public Interest Advocacy Centre; David Porter, Senior Solicitor at the Redfern Legal Centre; and Chris Watson, barrister from Forbes Chambers.

Abbreviations

- POI- person of interest
- GIPA/FOI- Government Information Public Access/ Freedom of Information
- PPIPA- Privacy & Personal Information Protection Act (NSW)
- LEPRA- Law Enforcement (Powers and Responsibilities) Act (NSW)

What is the COPS Database?

- *Name:* **C**omputerised **O**perational **P**olicing **S**ystem
- *Inception*: 1994
- *Description*: An operational database employed by the NSW Police to record all information related to offenders, victims and incidents that need police action
- *Purpose*: Police investigation and intelligence through the documentation of all incidents reported by victims or witnesses or matters becoming known to police which are assumed to require some police action
- *Common Uses*: Issuing charges, registering criminal incidents, intelligence gathering, ect.
- *Current Status:*
  - *1994*- Implemented COPS on ADABAS/Natural application hosted on an IBM mainframe
  - *2011*- Fujitsu hired to create 'WebCOPS'- a more modern web-based interface addition to original system to improve usability
  - *2014*- Incremental approach begun to upgrade system
  - *2015*- NSW Police called for tenders to engage in 'build phase' (replatforming) of upgrade

It was noted that a key factor to note when discussing the COPS database is that the system was designed to accommodate multiple databases and the multiple responsibilities of the NSW Police Force. An example was given of the firearms registry, and different levels of access to the breadth of information contained in the database. Two main aspects were identified that affect individuals: (1) the recording of events; and (2) the intelligence component that is also a part of the database. There is not much information about the Database on the public record. The intelligence component may include ostensibly minor details such as a report of someone who will provide alcohol to minors, or on the other end, extremely sensitive information regarding large scale importation. These details will not be

accessible to every sworn officer of the police force. A basic assumption exists that police officers should only access information on the database if it is related to their duties. This filters through on an individual officer's ability to access the different parts of the Database.

How do police make entries on the COPS database?

The NSW Council for Civil Liberties had made a general request to police as to whether the "audit trail" (ie, officers and ranks of those who viewed or mad entries in the database) could be accessed by the subject concerned. As a follow up with the police was met with no response, this sparked the question of what the policy of entries is.

It was noted that very little statutory guidance exists surrounding this. There does not seem to be a publicly available police policy on entries. Apparently, there are two guiding concepts: (1) that the database should contain all information that other officers need to perform their duty (once relevant to another officer it should be matter of record); and (2) every person on it is assigned a central names index (**CNI**) number. There is a very low threshold to meet these criteria, for example, a person giving information in respect of an assault will be given a CNI number.

Can a person access information held about them on the COPS Database?

Regarding the ability to access information through a GIPA application, this will be predominately from the standard COPS database regarding event reports. It is highly unlikely that a person can obtain intelligence reports unless a specific request is made and there is a clear public interest in disclosure.

The NSW GIPA does not tap into broad notions of accessing information, but rather applies a balancing test (for and against disclosure) set out in Act, which has been fairly narrowly construed in respect of the COPS Database. The balancing test contained in the GIPA in respect of information held by the police (in this case, the recording of an emergency '000' call) was decided by the Appeal Panel of the NSW Administrative Decisions Tribunal (as it then was) in *Commissioner of Police v Camilleri* [2012] NSWADTAP 19 . The Appeal Panel ruled that individual circumstances of the particular request are only relevant to the s.13 consideration (the presumption in favour of disclosure) under the GIPA. However, in considering s.14 (the presumption against disclosure) the agency (in this case, the police) and subsequently the Tribunal must only consider the administrative structure and context, and its (the administration's) conditions. The s.13 considerations must then be weighed against the s.14 considerations. In this sense, the s.14 considerations have primacy, or must first be considered (and again, not with regards to the particular facts of the case).

The GIPA test was most recently ruled on by the Appeal Panel of the NSW Civil & Administrative Tribunal in the case of *Commissioner of Police v Barrett* [2015] NSWCATAP 68. The case involved a dispute between neighbours. One of the neighbours attempted to obtain records, including the '000' recording and the 'audit trail' of entries on the COPS Database. The police refused the GIPA application. The applicant appealed to the NSW Civil & Administrative Tribunal, which found in favour of the applicant and ordered the police produce substantial amounts of information. The Appeal Panel of the Tribunal overturned this decision. The Applicant, Barret, argued that some specific considerations of the case must be attached to the s.14 (non-disclosure) consideration. The Appeal Panel disagreed, applying *Camilleri*.

It was noted that a subpoena was more likely to result in a positive response (than a GIPA), but a subpoena requires criminal or civil proceedings to be on foot.

What are the impacts of being on the COPS Database?

Being entered into the database can result in extra police attention. There have been cases of people being accused of breaching their bail conditions because of out-of-date entries. This has resulted in those people being arrested, taken into custody, searched and placed in a cell. The next morning these people have been taken to court. When the courts discovered that the database had not been updated, those people were told to go home from the Court. For some young people this has happened more than once. In one instance it happened to a young person three times in 15 days.

It was reported that one case concerned a man who had multiple event listings, as well as a list of alleged aliases. These aliases included a string of derogatory names referring directly to his sexuality. As any dealing in the future would bring up this string, this was affecting him. The names that had been entered into the system were brought to the attention of magistrate. The magistrate was outraged and made a recommendation that the names be removed, but whether that action was taken remains unknown.

Are COPS Database entries used in criminal trials?

There is an increasing trend to use Database entries in criminal trials. This was evident in a number of ways. First, according to s.33 of the Evidence Act, the statement on record is allowed to be read as evidence. If a problem exists regarding credibility of the entry and/or contamination, it may be too late in the sense that the jury or magistrate will have already digested the entry. The resources pressure on judicial officers is significant and they will likely dismiss objections to the evidence. But there are very few checks and balances to ensure an entry is properly made. Second, it seems that entries are used as a modern-day 'scrumdown', where the police witnesses look at the entry prior to the trial to "refresh their memory" of an event. In many matters, particularly in the local court, there are solely police witnesses. If this is the case, this is fundamentally a process where police are able to put their case together and share it.

It was observed that the COPS record often becomes the authoritative version of the police's view of events. There are, however, other more contemporaneous sources of police information: VHE police audio/radio is ordinarily accessible by subpoena (but may be redacted). In significant cases there is also **Eagle Eye**. Eagle Eye is an investigative database tool for significant investigations, recording exhibits, forensic material, and so on. It was noted that defendants should subpoena the Database and (if existent) the Eagle Eye records periodically throughout the course of an investigation/prosecution to see how these change. Regarding Catseye, there is a separate statutory privilege (against disclosure) attached to it.

What about false entries in the Database?

In *Turner v State of NSW* [2009] NSWDC, the plaintiff won a claim for damages for wrongful arrest. Partly to cover themselves, the arresting officers had falsified a COPS entry. The Court awarded aggravated and exemplary damages. The police officers were issued a reprimand.

One avenue to find information about the COPS Database is through police reprimands, internal investigations, employment disputes, and disciplinary hearings. One example

concerned a police officer who was assaulted off duty, and later looked up the COPS database entry about the incident and complained about the entry. He was investigated and prosecuted under restrictive information legislation. Information regarding such disciplinary matters may be able to be obtained by an applicant, if the applicant already has information which makes that relevant to the case at hand. (It is not necessarily fishing if the information is relevant to the matter.) This is one area where the complaints system can be useful. Police have been prosecuted under this section. Examples given of police officers gaining unauthorised access to COPS database, for instance individuals looking up ex partners new boyfriend/girlfriend, and an Ombudsman case of an officer looking himself up multiple times.

Will a refusal to give fingerprints be recorded on the database?

Yes, generally speaking, a refusal to cooperate with the police will be recorded on the database. There was a case which recorded a refusal to cooperate by a person. However, the entry failed to record that the individual was unconscious at the time of questioning. This illustrates the malleability of language, which can be used in interesting and devastating ways in a prosecution.

Is there a COPS database specific to vehicles?

Yes, NSW police are currently rolling out automatic number plate recognition to highway patrol vehicles and there is a funding push for this to be extended to local area commands. There was a recorded complaint of a man who was pulled over by police and asked to produce his license. When he inquired what the issue was, he was told that the vehicle had been noted as making a dangerous right turn a couple of months previously. This can have impacts on people who share cars, for instance.

Can a person amend COPS Database entries?

There is no entitlement to amendment of the database under s.15 of the PPIPA, s15, as identified in two cases:

- *ACP v Commissioner of Police, NSW Police Force* [2011] NSW ADT 249
- *Commissioner of Police, New South Wales Police Force v YK (GD)* [2008] NSW ADTAP 78

It was observed that attempts to amend the database via PPIPA or as a legal right had not been successful. In the ACP case, a woman had been charged and prosecuted for variety of domestic violence and child neglect cases and all were dismissed in the local court with costs. She rightly wanted as little information on the database as possible. The woman asked if mug shot, fingerprint, etc. be destroyed. Changes to the LEPRA left this option open for those whose cases were dismissed, or who had been acquitted. When requested to do so, police replied they could not because of the *State Records Act*. When this legislation was amended, it only allowed fingerprints to be removed but not mug shots. This is an unsatisfactory state of affairs; it is misleading and gives the impression that the custody was for a legitimate purpose, or that the individual is a criminal.

Under PPIPA, police have an immunity from privacy requirements except in relation to educative and some other functions. The entries of mug shots and fingerprints should be classified as an administrative function, and people should be entitled to request amendment or removal under the PPIPA

What about where there has been incorrect or contaminated entries?

As noted, there is no legal entitlement to amend the database. However, there has been some success in changing or removing entries in cases where specific issues can be raised, for example, if an entry is leading to a waste of police resources, or causing unfairness to a particular individual. The police ought be approached at the first instance, and then the Ombudsman if that is unsuccessful.

Is it possible to challenge COPS Database entries on the grounds of defamation?

This issue was dealt with at least tangentially in the case of *Giovennetti v State of NSW* [2013] NSWSC 1960. A man joined a gym, then had his membership revoked on the basis of an email by a police officer, which was based in part on COPS Database entries. The email was the subject of defamation proceedings. Ultimately, the plaintiff was unsuccessful on grounds of qualified privilege (the police officer was entitled to send on the information in accordance with statutory duties). NOTE: The CCL has subsequently been informed that this particular complainant made a complaint to the Ombudsman about his COPS Database entries, and the particular entries in question were removed after a recommendation by the Ombudsman.

Can COPS entries be made on interstate people?

Yes absolutely, it doesn't need to refer back to official identity document in legitimate cases of aliases. In practice, you could get order to get destroyed, they simply keep a copy.

Audience Member Comment: Spoke regarding a case in 2000 involving police refusal to amend intelligence reports. Discussed the applicability of the Freedom of Information Act in relation to the case. Mentioned that the police appeal lost.

Is the COPS database not fundamentally about preventative policing? And is this not legitimate, particularly in areas such as terrorism or paedophilia? Would the police not argue that crime rates are down?

There is a legitimate purpose for the police to have the database. However, a real danger exists if there are inadequate checks and balances within the system. The fundamental concern is that the database and entries be accurate. There are many cases of people being subjected to stop and searches based on the database, where the database is wrong.

Is the COPS Database just proactive policing, and is that not a good thing?

There is a real danger of snowballing once a person has been entered into the system. However, there is a legitimate argument that it is better that there is a police record than not. Even though an individual could end up with lots of entries, it might be preferable that there is a record, than nothing at all.

What would be an appropriate oversight mechanism?

An appropriate audit trail which shows who view and amended records is needed, to ensure that changes to entries can be monitored over time. A further change needs to occur in the mindset of ordinary officers, and in particular for them to be more sceptical of the database. The fallout from Operation Mascot has illustrated to the police the devastating toll that bad intelligence can take. There is at present an opportunity for change in NSW.