

# REPORT OF THE INTEGRITY COMMISSION

**No. 3 of 2018**

---

Report of an own-motion  
investigation into the  
management of information in  
Tasmania Police



---

The objectives of the Integrity Commission are to –

- improve the standard of conduct, propriety and ethics in public authorities in Tasmania;
- enhance public confidence that misconduct by public officers will be appropriately investigated and dealt with; and
- enhance the quality of, and commitment to, ethical conduct by adopting a strong, educative, preventative and advisory role.

© Integrity Commission 2018

This report and further information about the Commission can be found on the website

[www.integrity.tas.gov.au](http://www.integrity.tas.gov.au)

GPO Box 822,  
Hobart  
Tasmania 7001

Phone: 1300 720 289

Email: [integritycommission@integrity.tas.gov.au](mailto:integritycommission@integrity.tas.gov.au)

ISSN 2204-5910 online

ISSN 2204-5902 print

President  
Legislative Council  
Parliament House  
HOBART 7000

Speaker  
House of Assembly  
Parliament House  
HOBART 7000

Dear Mr President

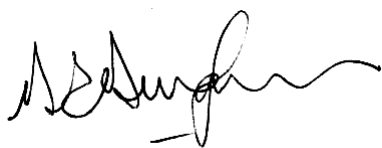
Dear Madam Speaker

Pursuant to section 11(3) of the *Integrity Commission Act 2009* (the Act), the Integrity Commission presents *Report 3 of 2018* to Parliament, arising from an own-motion investigation into the management of information in Tasmania Police.

Yours sincerely,



**Aziz Gregory Melick AO RFD SC**  
Chief Commissioner  
On behalf of the Board



**Richard Bingham**  
Chief Executive Officer

14 June 2018

This page intentionally left blank.



## **OWN-MOTION INVESTIGATION REPORT**

**An own-motion investigation into the  
management of information in Tasmania Police**

**Finalised following submissions received under  
section 56(1) of the *Integrity Commission Act 2009***

**6 June 2018**

---

# Contents

---

Glossary, legislation and acronyms .....	iii
Executive summary .....	iv
1. Introduction .....	1
2. A matter of trust: the use and abuse of public sector information.....	7
3. Penalties for public sector abuse of information.....	11
4. Policies and procedures on information management .....	23
5. Information security policies, practices and procedures.....	32
6. Culture and training .....	38
7. Investigating and penalising abuse of information .....	42
8. Concluding remarks.....	51
Appendix A – References .....	52
Appendix B – Information abuse offences across Australia .....	59
Appendix C – Submission of Tasmania Police .....	62
Appendix D – Submission of Director of Public Prosecutions .....	63
Appendix E – Submission of Police Association of Tasmania .....	64

## Glossary, legislation and acronyms

---

<b>AFP:</b>	Australian Federal Police
<b>Commission:</b>	Integrity Commission
<b>Criminal Code:</b>	<i>Criminal Code Act 1924</i> (Tas) sch 1
<b>DPFEM:</b>	Department of Police, Fire & Emergency Management ('the Department')
<b>Employee:</b>	When the word 'employee' is used in this report, it is a reference to all employees of Tasmania Police, not just police officers
<b>IAPro:</b>	The database used by Tasmania Police to manage police conduct
<b>IC Act:</b>	<i>Integrity Commission Act 2009</i> (Tas)
<b>MIPO:</b>	The criminal offence of 'misconduct in public office'; MIPO may have a different name depending on the jurisdiction, for example: misfeasance in office, misbehaviour in public office, and abuse of public office
<b>Officer:</b>	A 'police officer', as defined in section 3 of the <i>Police Service Act 2003</i> (Tas)
<b>PIP Act:</b>	<i>Personal Information Protection Act 2004</i> (Tas)
<b>PS Act:</b>	<i>Police Service Act 2003</i> (Tas)
<b>QPS:</b>	Queensland Police Service
<b>Queensland CCC:</b>	Crime and Corruption Commission Queensland.
<b>TPM:</b>	Tasmania Police Manual, as published in accordance with section 93 of the <i>Police Service Act 2003</i> (Tas)
<b>WAPOL:</b>	Western Australia Police
<b>West Australian CCC:</b>	Corruption and Crime Commission Western Australia

## Executive summary

---

This is a report of an own-motion investigation by the Integrity Commission (the Commission) into the policies, practices and procedures of Tasmania Police in relation to unauthorised access to, and misuse of, information by police officers.

As an own-motion investigation, it was not triggered by a complaint but by the Commission's recognition, along with similar jurisdictions interstate, that significant advances in technology have increased the risk of information abuse within the public sector. The broad purpose of the investigation was to better understand how Tasmanian public sector organisations manage information and associated risks, enabling greater focus on good practice.

Tasmania Police was selected as the subject of the investigation because its work, to a greater degree than many other public sector organisations, relies on information. The abuse of information by public sector employees has the capacity to significantly erode public trust. It can also impact adversely on the work of an organisation, and in some situations may be a threat to safety. It is essential to police credibility that information is adequately protected from unauthorised access and use.

It is also the job of police to investigate potentially criminal allegations against other public sector employees. In some respects, Tasmania Police is the gatekeeper for the appropriate management of serious information abuse by Tasmanian public sector employees more generally.

This report includes a review of options for penalising information abuse across Australia. The review indicates that in Tasmania, options for prosecuting serious information abuse by public sector employees are more limited than in other jurisdictions. The Commission has determined that it is a matter for the Parliament of Tasmania as to whether this should be changed. We have, however, made one specific recommendation for legislative review.

The report also describes good practice management of information by the public sector, and examines Tasmania Police policies, practices and procedures. It explains that organisations should have simple and clear policies and procedures, adequate information security measures, and should cultivate good organisational culture and awareness. Public sector organisations must also be prepared to enforce their policies and procedures, through either the disciplinary or legal system as appropriate.

This investigation has found that, overall, Tasmania Police policies, practices and procedures are adequate and appropriate. This is reliant on Tasmania Police maintaining its current focus on information management. Areas in which the organisation is to be particularly commended are the processes used in the ongoing audits of access to information, the newly drafted clause in the Tasmania Police Manual and the new conduct and complaints management system, '*Abacus*'.

While the investigation found that in most respects Tasmania Police meets good practice standards, we have made some specific suggestions for improvements. The most important suggestion is that the organisation should be more prepared to enforce its policies and procedures when investigating alleged information abuse.

Finally, it is important to note that while this investigation was thorough, independent and undertaken with the full cooperation of Tasmania Police, it was limited in two respects: we



did not survey all police officers and thus did not obtain a complete picture of police views on this issue; and we do not have direct and independent access to the Tasmania Police complaints database.

#### **Recommendation no. 1**

It is recommended to the Premier that Tasmania's 'Disclosure of official secrets' and 'Unauthorized access to a computer' offences be reviewed, with a view to amending them to make the law more certain, and/or to align them with equivalent offences in other Australian jurisdictions.

The offences referred to are in sections 110 and 257D of schedule 1 of the *Criminal Code Act 1924* (Tas) and section 43C of the *Police Offences Act 1935* (Tas).



# 1. Introduction

---

## 1.1. Background

- [1] The last thirty years have seen significant advances in technology, and a corresponding increase in public sector reliance on – and access to – personal and sensitive information.
- [2] In the modern world, information abuse is a risk in all public sector organisations. Information abuse is when an employee either accesses information to which they are not entitled, or misuses information gained by virtue of their employment.<sup>1</sup> Most public sector employees have the capacity to abuse information in some respect.
- [3] Information abuse can have serious adverse ramifications for organisations, not least because of the potential for the erosion of public trust. Abuse of information by public sector employees is therefore a source of continuing focus for integrity agencies across Australia.
- [4] The Integrity Commission (the Commission) had for some time considered that it should investigate how Tasmanian public sector organisations manage information and allegations of information abuse by their employees.

### **Why Tasmania Police?**

- [5] Although this report will be valuable for many public sector organisations, its focus is on Tasmania Police.
- [6] Police organisations are more reliant on information, and on their employees handling information appropriately, than most public sector organisations. From its annual audits of police complaints, the Commission had identified that this may be an issue that could be handled better by Tasmania Police.
- [7] The Commission has conducted four full annual audits of complaints against police.<sup>2</sup> For a range of reasons, we decided that in future these audits would be conducted less frequently, and that the Commission would occasionally undertake own-motion investigations into particular police misconduct issues. We decided that the first of these own-motion investigations would be into allegations of unauthorised access to, and misuse of, information.
- [8] The way in which Tasmania Police views information abuse is important not only in terms of the police service itself, but for the entire Tasmanian public sector. This is because it is not only police that have access to personal and sensitive information. For example, employees in Transport (part of the Department of State Growth) and in the Tasmania Prison Service (part of the Department of Justice) also have access to this kind of information.

---

<sup>1</sup> Terminology about abuse of public sector information may vary depending on the circumstances. For the sake of simplicity, this report uses the phrases 'unauthorised access to information' and 'misuse of information'. The term 'information abuse' is used as a global phrase to cover both unauthorised access to, and misuse of, information.

<sup>2</sup> These reports can be access on our website at <[www.integrity.tas.gov.au/reports\\_and\\_publications/reports](http://www.integrity.tas.gov.au/reports_and_publications/reports)>.

- [9] As with police employees, if other public sector employees are accused of information abuse and referred to Tasmania Police for investigation, the allegations should be taken seriously and pursued where appropriate. This means that, in some respects, Tasmania Police is the gatekeeper for the appropriate management of serious information abuse by Tasmanian public sector employees more generally.
- [10] It is therefore necessary that the police service has a good understanding of the importance and sensitivity of public sector information, and of when it is appropriate to prosecute an employee or former employee.

### **Determination to conduct an own-motion investigation**

- [11] On 15 June 2017, the then acting chief executive officer (CEO) of the Commission determined to commence an own-motion investigation in accordance with section 89(1)(c) of the *Integrity Commission Act 2009* (Tas) (*IC Act*),

*into the policies, practices or procedures, or the failure of those policies, practices or procedures, of Tasmania Police in relation to unauthorised access to, and/or misuse of, information by persons in the Police Service.*

### **Jurisdiction**

- [12] It is a principal objective of the Commission to appropriately investigate and deal with allegations of misconduct. In the performance of its functions and exercise of its powers, the Commission may inform itself of any matter in such a manner as it thinks fit. In this matter, the Commission's jurisdiction was invoked on delegation from the Board to the CEO to undertake policy, practice and procedure own-motion investigations.
- [13] An own motion-investigation into police misconduct is defined in section 89 of the *IC Act* to include an investigation into any of the policies, practices or procedures of Tasmania Police in relation to misconduct. During any investigation, the investigator may make any investigations he or she considers appropriate, may conduct the investigation in any lawful manner he or she considers appropriate, and may obtain information from any persons in any lawful manner he or she considers appropriate: section 46 of the *IC Act*.
- [14] The conduct of the investigation was carried out in accordance with section 47 of the *IC Act*.

### **Aim**

- [15] The aim of the own-motion investigation was:
1. to gain an understanding of:
    - a. how Tasmania Police manages access to information
    - b. how Tasmania Police responds to alleged unauthorised access and/or misuse of information by its officers and
    - c. good practice in relation to management of access to information in police services, and

2. to identify if and what improvements could be made in Tasmania Police policies and practices in relation to management of information.

## **Scope**

[16] The scope of the investigation was:

- legislation, records, information and material relating to management of access to information within Tasmania Police
- allegations of unauthorised access and/or misuse of information by Tasmania Police officers, and
- the understanding and attitudes of Tasmania Police officers, both senior and junior, to management of access to information and allegations of unauthorised access to and/or misuse of information by Tasmania Police officers.

[17] The source of the Commission's power to conduct an own-motion investigation into police misconduct matters (under section 89 of the *IC Act*) is different to the source of its power to conduct an own-motion investigation into other public authorities (under section 45 of the *IC Act*).

[18] The investigation was limited to police officers appointed to the 'Police Service' as defined in section 4 of the *Police Service Act 2003* (Tas) (*PS Act*). It did not include Tasmanian State Service employees employed under the *State Service Act 2000* (Tas) who work in Tasmania Police or in the Department of Police, Fire and Emergency Management (DPFEM).

## **Limits of the investigation**

[19] This investigation was limited in two respects.

### *Direct access to Tasmania Police complaints databases*

[20] The Commission does not have direct access to the Tasmania Police complaints database, IAPro. The Commission has previously noted that this is a limitation on its ability to oversight police generally,<sup>3</sup> and acknowledges there are a number of legal issues that restrict us from directly accessing IAPro.<sup>4</sup>

[21] The Commission's inability to access IAPro directly meant that it was reliant on Tasmania Police supplying information about information abuse allegations. While Tasmania Police maintained a high level of cooperation and provided all information requested by the Commission, the lack of direct access meant it was possible that we did not get every relevant file. This is due to our requests being related to specific

---

<sup>3</sup> Integrity Commission, Submission to Independent Review, *Integrity Commission Act Review*, March 2016, 44–5 <[www.integrity.tas.gov.au/reports\\_and\\_publications/reviews](http://www.integrity.tas.gov.au/reports_and_publications/reviews)>; Integrity Commission, *Submission to the Three Year Review* (2013), volume 1, 112–115 <[www.integrity.tas.gov.au/reports\\_and\\_publications/reviews](http://www.integrity.tas.gov.au/reports_and_publications/reviews)>.

<sup>4</sup> Integrity Commission, Submission to Independent Review, *Integrity Commission Act Review*, March 2016, 44–5 <[www.integrity.tas.gov.au/reports\\_and\\_publications/reviews](http://www.integrity.tas.gov.au/reports_and_publications/reviews)>; Integrity Commission, *Submission to the Three Year Review* (2013), volume 1, 112–115 <[www.integrity.tas.gov.au/reports\\_and\\_publications/reviews](http://www.integrity.tas.gov.au/reports_and_publications/reviews)>.

allegation types yet there is an element of fluidity to allegation categorisation within the Tasmania Police database,<sup>5</sup> and our previous audits of police complaint files have noted that the database records may not always be accurate.<sup>6</sup>

- [22] One option put forward by the Commission was that Tasmania Police could have facilitated our access by allowing a Commission investigator to be appointed an ‘ancillary constable’ under the *PS Act*. However this suggestion was not adopted by Tasmania Police.

#### *Survey of police officers*

- [23] The Commission had intended to conduct a survey of police officers as part of this investigation. To ensure the survey results would be as independent as possible, we contracted a local company to undertake the survey.
- [24] Tasmania Police was accepting of the survey, and we liaised with senior police to draft the questions.
- [25] The survey would have provided a better understanding of information management in regard to:
- whether police have a good understanding of their responsibilities
  - culture
  - the adequacy of training, awareness initiatives and support provided to officers
  - whether officers believe policies, procedures and practices are adequate and appropriate, and
  - whether the views of police officers differ according to age, length of time in the service, or rank.
- [26] The Commission met with the Police Association of Tasmania to discuss the survey; a draft copy of the survey was supplied.
- [27] Despite its acceptance by Tasmania Police, the Police Association advised that although it would not actively campaign against the survey, if officers asked, they would be advised that the Association did not support it. The Association was uncomfortable about the questions in the survey and could see no reason for the investigation to be conducted, or why its focus should be on Tasmania Police.
- [28] The Commission determined that, without the support of the Police Association, the survey was very unlikely to get enough responses for valid data to be obtained and consequently did not conduct the survey.
- [29] The Commission met with a number of senior police to discuss matters such as police culture around access to information, and their views are reflected in this report.

---

<sup>5</sup> For a discussion about some aspects of this, see Integrity Commission, *An audit of Tasmania Police complaints finalised in 2013*, Report No. 2 (2014) 19; Integrity Commission, *An audit of Tasmania Police complaints finalised in 2014*, Report No. 2 (2015) 32; Integrity Commission, *An audit of Tasmania Police complaints finalised in 2015*, Report No. 1 (2016) 5, 32.

<sup>6</sup> Integrity Commission, *An audit of Tasmania Police complaints finalised in 2013*, Report No. 2 (2014) 14–16; Integrity Commission, *An audit of Tasmania Police complaints finalised in 2014*, Report No. 2 (2015) 32–3; Integrity Commission, *An audit of Tasmania Police complaints finalised in 2015*, Report No. 1 (2016) 30–3.

However given their seniority and that most were based within Professional Standards Command, the views of these officers are not necessarily representative of the views of the average police officer. The Police Association declined an opportunity to meet with the Commission to put its members' views forward.

## **1.2. Conduct of the investigation**

[30] The process followed by the Commission in this investigation was, in rough chronological order:

1. notifying the Commissioner of Police about the investigation, and requesting the appointment of a contact officer and the provision of relevant policies and procedures
2. research into legislation, policies, practices, reports and legal cases from Tasmania and other jurisdictions
3. designing a survey instrument, including contracting a company and liaising with police and Police Association representatives (as discussed above, this survey did not eventuate)
4. obtaining and auditing Tasmania Police records about information abuse allegations, and
5. meetings with police representatives from Professional Standards Command and the Police Academy.

### **Coercive powers and confidentiality**

[31] Tasmania Police cooperated with the Commission throughout the course of the investigation.

[32] The Commission did not use its coercive powers and did not apply formal *IC Act* confidentiality requirements to any aspect of the investigation.

### **Meetings and engagement**

[33] As part of this investigation, the Commission met with a number of Tasmania Police officers to discuss unauthorised access to and misuse of information. This included, from Professional Standards Command, two sergeants, two inspectors and the Commander. We also met with an inspector from the Police Academy, and the Deputy Commissioner was contacted at a number of points.

[34] Matters discussed at these meetings included:

- historical attitude and culture of Tasmania Police and its officers toward information management
- current culture and practice around information management
- the framework governing information management
- Tasmania Police audits of officer access to information
- how allegations of information abuse are managed

- files audited by the Commission as part of this investigation, and
- recruitment processes, training and education.

### **Procedural fairness**

- [35] A draft of this report was provided to Tasmania Police, the Police Association of Tasmania and the Director of Public Prosecutions ('DPP') under section 56 of the *IC Act*, on 18 April 2018. This provided an opportunity for those parties to make comments or submissions on the content of the report, including any proposed findings or recommendations.
- [36] During this period, the Commission met with the DPP to clarify potential issues that the DPP felt may warrant his attention. Based upon this meeting, the Commission forwarded proposed new wording of certain sections of the report.
- [37] Submissions were received from all three parties, and are attached in full to this report (Appendices C–E).

### **1.3. Structure of this report**

- [38] This report is divided into six chapters that:
1. explain information abuse and its prevalence
  2. set out potential penalties for public sector information abuse in Tasmania and other Australian jurisdictions
  3. discuss policies and procedures on information management, including good practice and what happens in other police jurisdictions and Tasmania Police
  4. cover good practice and Tasmania Police information security policies, practice and procedures
  5. discuss culture and training in other jurisdictions, in Tasmania Police, and good practice, and
  6. look at how allegations of information abuse should be managed, and how they are managed by Tasmania Police.



## **2. A matter of trust: the use and abuse of public sector information**

---

### **2.1. What information do public sector organisations hold?**

- [39] All public sector organisations hold information that is vulnerable to abuse by their employees. This usually includes information about clients and other members of the public; the organisation's employees; and the work and functions of the organisation.
- [40] Information is vital to the work and functions of law enforcement agencies such as police services. Key information held by a police service or accessible to its employees includes:
- criminal and arrest records
  - personnel records
  - vehicle registration details
  - records related to investigations
  - informant details, and
  - reports and information passed on by other police services.
- [41] Public sector organisations, including police services, do not 'own' the information they hold; rather, they are the guardians of the information. The public has entrusted the organisation and its employees with the information on the understanding that it will be accessed and used only in the course of official duties.

### **2.2. What is abuse of information?**

- [42] Employees do not have a right or entitlement to access and use information held by their organisation as they personally wish. That would be abuse of information, which may be categorised as either unauthorised access to information, or misuse of information.
- [43] 'Unauthorised access to information' occurs when a public sector employee accesses information available to them through their work for personal – not professional – reasons. It may include, for example, looking up friends, family members and potential partners on a database.
- [44] 'Misuse of information' occurs when a public sector employee mistreats information gained through their work. Examples of 'misuse of information' include:
- leaking information to the media
  - inadvertent or careless loss of data
  - sharing sensitive information on social media
  - preying on vulnerable persons met at work
  - using information to harass or bully another employee

- adding false information to public sector records, and
- exchanging confidential information for money or other benefits.

[45] Misuse of information is not always done to gain a financial or tangible benefit. It is just as possible for the motivation to be something intangible, such as ego, voyeurism, excitement, altruism, or malicious intent. Misuse of information may also be inadvertent or unintentional – for instance when the employee’s judgment is impaired due to overconsumption of alcohol, or when a laptop is misplaced.

### **Predatory behaviour and preying on vulnerable persons**

An area of particular concern is the use of information to facilitate predatory behaviour, or to prey on vulnerable persons. Examples of predatory behaviour include obtaining contact details for a person the employee is attracted to from a work database, or pursuing a relationship with a vulnerable person encountered during the course of official duties. This is most likely to occur in public sector jobs where employees frequently have contact with vulnerable members of the public. This includes employees such as social and hospital workers, and police officers.

In Victoria, the Independent Broad-based Anti-corruption Commission (IBAC) has found that the misuse of police databases is likely to be a ‘key component’ in predatory police behaviour.<sup>7</sup> Every single case study in a report from the England and Wales police complaints oversight body on the use of police powers to perpetrate sexual violence involved some kind of misuse of information.<sup>8</sup>

## **2.3. Risks**

[46] Public sector organisations should be ‘fully aware of all the personal information they handle, where it is kept and risks associated with that information’.<sup>9</sup>

[47] Abuse of information may be a serious breach of privacy, and can have many adverse outcomes. These include:

- erosion of public trust in the public sector
- damage to the reputations of individuals and organisations
- the facilitation of – and increasing the likelihood of the employee progressing to – other forms of misconduct, corruption and crime (the ‘slippery slope’)
- providing an unfair advantage to the recipients of the information, and placing a financial burden on the organisation, and
- undermining the ability of public sector organisations to perform their functions.

<sup>7</sup> Independent Broad-based Anti-Corruption Commission, *Predatory behaviour by Victoria Police officers against vulnerable persons: Intelligence report 2* (December 2015) 9.

<sup>8</sup> Independent Police Complaints Commission, *The abuse of police powers to perpetrate sexual violence* (September 2012).

<sup>9</sup> David Smith and Tim Lee, ‘When there is a breach – Know your obligations and what steps to take’ (2015) 88 *Computers & Law* 1, 6.

- [48] The potential adverse outcomes for police services are even greater than most other public sector organisations. It can, for example, result in a reluctance on the part of informants and other law enforcement agencies to share information. It can also damage the outcomes of investigations and prosecutions, and place people in danger. As stated by the former Victorian Office of Police Integrity, police 'credibility in large part rests on its ability to protect the information it gathers and holds and to conduct investigations free from compromise and disruption by organised crime and, in some instances, corrupt police officers'.<sup>10</sup>
- [49] In terms of information held by police services, the critical risk assessment factors of opportunity, vulnerability and the possibility of dire consequences are all present.<sup>11</sup> Information management should therefore be a key focus of police services.

## 2.4. How common is abuse of public sector information?

- [50] Complaint statistics are of limited usefulness in quantifying the prevalence of this conduct across the public sector, as often the victim is oblivious and therefore not in a position to complain.<sup>12</sup> The conduct is – especially in the case of misuse of information – difficult to detect and to prove, so complaint substantiation rates are also not a reliable indicator.<sup>13</sup>
- [51] Nonetheless, it can be one of the most common allegations against public sector employees.<sup>14</sup> This is particularly so for police services. In a recent survey of Victoria Police employees, misuse of information was identified as one of five areas with the greatest opportunity for corruption to occur. Eighty-seven percent of police respondents agreed that there was opportunity for misuse of information to occur – compared with 61% of local government respondents and 56% of state government respondents.<sup>15</sup>
- [52] Victoria Police employees also rated misuse of information as one of three behaviours that was 'considered most likely to have been suspected of occurring, and most likely to have been observed'.<sup>16</sup>

---

<sup>10</sup> Office of Police Integrity Victoria, *Investigation into Victoria Police's Management of the Law Enforcement Assistance Program (LEAP)* (March 2005) 34.

<sup>11</sup> Criminal Justice Commission Queensland, *Protecting Confidential Information: A Report on the Improper Access to, and Release of, Confidential Information from the Police Computer Systems by Members of the Queensland Police Service* (November 2000) 39.

<sup>12</sup> Criminal Justice Commission Queensland, *Protecting Confidential Information: A Report on the Improper Access to, and Release of, Confidential Information from the Police Computer Systems by Members of the Queensland Police Service* (November 2000) 30; Julie People, 'Research and Issues Papers Number 02: Unauthorised Disclosure of Confidential Information by NSW Police Officers' (October 2008) *Police Integrity Commission New South Wales* 2.

<sup>13</sup> Criminal Justice Commission Queensland, *Protecting Confidential Information: A Report on the Improper Access to, and Release of, Confidential Information from the Police Computer Systems by Members of the Queensland Police Service* (November 2000) 30.

<sup>14</sup> Crime and Corruption Commission Queensland, *Confidential information: Unauthorised access, disclosure and the risks of corruption in the Queensland public sector* (May 2016) 1.

<sup>15</sup> Independent Broad-based Anti-Corruption Commission, *Perceptions of corruption: Survey of Victoria Police employees* (December 2017) 7.

<sup>16</sup> Independent Broad-based Anti-Corruption Commission, *Perceptions of corruption: Survey of Victoria Police employees* (December 2017) 4.

[53] At the Commission, in the four years to 30 June 2017, approximately:

- 13% of all complaints and notifications about any public sector employee contained one or more allegations of information abuse, and
- 15% of complaints and notifications about Tasmania Police officers contained one or more allegations of information abuse.

### 3. Penalties for public sector abuse of information

---

- [54] The unauthorised access to or misuse of information by public sector employees may, in certain circumstances, be pursued through disciplinary avenues, be a breach of legislation, or amount to an offence or a crime.

#### 3.1. Disciplinary avenues

- [55] Abuse of information is most often pursued as a disciplinary (misconduct) matter, rather than as an offence. This can be for a range of reasons, including because the conduct is less serious and does not warrant the resources required for a prosecution. It can also be because of difficulties in proving these kinds of offences, for example due to the specific requirements of the offence, or because of a lack of policy or policy enforcement in the organisation.
- [56] There are a range of ways in which abuse of information could amount to misconduct. In Tasmania Police, 'misconduct' is a breach of the Code of Conduct, which is set out in section 42 of the *PS Act*.<sup>17</sup>
- [57] Tasmania Police processes for dealing with allegations of a breach of the Code of Conduct are set out on its website.<sup>18</sup> Potential outcomes for sustained breaches range from no action, to professional development measures only, up to sanctions as set out under section 43(3) of the *PS Act*. A sanction may be anything from a 'counselling' up to termination of employment.

#### Misconduct under the Integrity Commission Act

- [58] The *IC Act* definition of 'misconduct' specifically includes information abuse. Under section 4 of the *IC Act* (emphasis added)

*misconduct means –*

*(a) conduct, or an attempt to engage in conduct, of or by a public officer that is or involves –*

*(i) a breach of a code of conduct applicable to the public officer; or*

*(ii) the performance of the public officer's functions or the exercise of the public officer's powers, in a way that is dishonest or improper; or*

*(iii) a misuse of information or material acquired in or in connection with the performance of the public officer's functions or exercise of the public officer's powers; or*

*(iv) a misuse of public resources in connection with the performance of the public officer's functions or the exercise of the public officer's powers; or*

*(b) conduct, or an attempt to engage in conduct, of or by any public officer that adversely affects, or could adversely affect, directly or indirectly, the*

---

<sup>17</sup> The sections of the Code of Conduct most relevant to information are *Police Service Act 2003* (Tas) ss 42(4), (7), (8), (9) and (10).

<sup>18</sup> Tasmania Police, *Abacus: Police Conduct & Complaint Management* (December 2017) About Us <[www.police.tas.gov.au/about-us/abacus/](http://www.police.tas.gov.au/about-us/abacus/)>.

*honest and proper performance of functions or exercise of powers of another public officer –*

*but does not include conduct, or an attempt to engage in conduct, by a public officer in connection with a proceeding in Parliament;*

- [59] This means that, aside from any potential breaches of the Code of Conduct applicable to a public sector employee, the Commission has specific jurisdiction over the alleged misuse of information.

### **3.2. Privacy and other legislation**

- [60] The unauthorised access to or misuse of information may be a breach of privacy legislation. The relevant Tasmanian legislation is the *Personal Information Protection Act 2004* (Tas) ('*PIP Act*').
- [61] A breach of the *PIP Act* is committed by an organisation, not an individual. A person may make a complaint about a breach of the *PIP Act* to the Ombudsman. If, after an investigation, the Ombudsman finds there has been a breach, this must be reported to the relevant Minister, who must then table information about the breach in Parliament.<sup>19</sup>
- [62] There may also be legislation specific to the kind or type of information that was accessed or shared. For instance, there is specific legislation about the confidentiality of health records, and there are offences for breaches of legislation such as the *Telecommunications (Interception and Access) Act 1979* (Cth).

### **3.3. Crimes and offences**

- [63] Unauthorised access to and misuse of information by public sector employees is most likely to be a crime or an offence under one of the following categories:
- computer hacking, or unauthorised access to information
  - official corruption or bribery
  - disclosure of official secrets, or
  - misconduct in public office.
- [64] It may also be a crime or an offence under legislation specific to the organisation. A table setting out offences across Australian jurisdictions is in the appendix of this report.

#### **Computer hacking or unauthorised access to information**

- [65] All Australian jurisdictions have some form of summary or criminal offence for unauthorised access to information or computer 'hacking'.<sup>20</sup> Most of these offences could be applied – theoretically – to public sector employees using work systems to

---

<sup>19</sup> *Personal Information Protection Act 2004* (Tas) s 22.

<sup>20</sup> Although some of these offences are called 'computer hacking', most do not require hacking in the traditional sense of the word.

access information to which they are not entitled. These offences apply when the access itself is unauthorised, and do not require the gaining of a benefit or the causing of a detriment. That is, they do not require the information to be used by the employee.

[66] The prosecution guidelines published by the DPP concerning computer-related crime contain the following:

*Care must be taken to choose a charge which reflects the nature and extent of the criminal conduct disclosed by the evidence which will enable a court to impose a sentence commensurate with the gravity of the conduct.*

*These guidelines are to assist prosecutors in the exercise of their discretion. Each case should be approached and assessed on its merit.*

*Where the computer-related crime involves fraud a similar approach to stealing as provided by s 72 of the Justices Act 1959 should be taken. That is, a summary charge should be preferred where the amount of the alleged computer-related fraud is less than \$20,000 unless:*

- *the charge involved forms part of a course of conduct or series of crimes which are indictable*
- *circumstances relating to the alleged offender and/or to the conduct are such that the penalty provision in the lower court would not be adequate*
- *a co-accused was dealt with on indictment (prosecutors should strive for consistency as between co-offenders unless there are compelling reasons not to).*

*Where the crime does not involve a financial element, such as damaging data or inserting false information for non-financial reasons, in determining whether a charge should be summary or indictable the purpose of the crime and its result should be considered. Generally the charge should be a summary one unless the conduct involves serious, or potentially serious, risk to lives or property.*

*Similarly, in the case of unauthorised access to a computer, consideration needs to be given to the type of information accessed and the purpose of the access.*

*Before any charges, whether summary or indictable, are laid further consideration needs to be given as to whether the conduct may be adequately dealt with by employment codes of conduct.*

*In determining whether an employment code of conduct is sufficient, regard to the following is required:*

- *The type of material accessed.*
- *The purpose for which it was accessed, e.g. was it for a malicious purpose?*
- *Whether the material was disseminated.*
- *Whether the access caused any actual harm to an individual or organisation.*

- *The likely penalty pursuant to a code of conduct proceeding.*<sup>21</sup>

[67] As noted by the Commonwealth Director of Public Prosecutions, even where an incident could be prosecuted under this kind of legislation, it is not always in the public interest to do so. Instructions from that office state that:

*2.2 in determining where the public interest lies, it is relevant to have regard to the public interest in protecting confidential information and in showing that the misuse of confidential information will be treated seriously;*

*2.3 it is also relevant to have regard to the offender's motives (whether they can be formally proved or not) and the impact (if any) on the person to whom the information relates;*

*2.4 as a general rule prosecution will be the appropriate response in any case where the offender acted for financial, commercial or political gain; for the purpose of adversely affecting the operations of the agency; or for the purpose of causing harm, loss or prejudice to another person.*<sup>22</sup>

[68] In 2000 the Criminal Justice Commission (now the Crime and Corruption Commission) stated that no unauthorised access offence existed at that time in Queensland, and that – given the existence of disciplinary provisions – it did not recommend enacting such an offence.<sup>23</sup> However, section 408E of the *Criminal Code Act 1899* (Qld) – titled ‘computer hacking and misuse’ – has been used to charge a number of police officers in recent years.<sup>24</sup> For example, in 2016 a former detective was fined \$8,000 for accessing ‘the Queensland Police database to find the phone numbers of men to send “personal” text messages and arrange meetings’.<sup>25</sup>

[69] A string of police officers and other public sector employees have also been charged under the equivalent provision in Western Australia – section 440A of the *Criminal Code Act Compilation Act 1913* (WA). Examples include:<sup>26</sup>

<sup>21</sup> Tasmanian Director of Public Prosecutions, *Prosecution Policy and Guidelines*, available at [http://www.dpp.tas.gov.au/prosecution\\_obligations/prosecution\\_policy\\_and\\_guidelines](http://www.dpp.tas.gov.au/prosecution_obligations/prosecution_policy_and_guidelines), retrieved on 9 May 2018.

<sup>22</sup> Commonwealth Director of Public Prosecutions, *Practice Group Instruction Number 2: Computer Browsing offences under the Criminal Code* (3 September 2014) <[www.cdpp.gov.au/crimes-we-prosecute/general-prosecutions](http://www.cdpp.gov.au/crimes-we-prosecute/general-prosecutions)>. Note that this is in regard to the Commonwealth legislation, which is in *Criminal Code Act 1995* (Cth) s 478.1.

<sup>23</sup> See Criminal Justice Commission Queensland, *Protecting Confidential Information: A Report on the Improper Access to, and Release of, Confidential Information from the Police Computer Systems by Members of the Queensland Police Service* (November 2000) 105.

<sup>24</sup> Crime and Corruption Commission Queensland, ‘Police officer charged for unauthorised access and disclosure of confidential information - 22 June 2016’ (Media Release, 22 June 2016); Crime and Corruption Commission Queensland, ‘CCC serves Brisbane policeman with a notice to appear in court for misusing database - 13 June’ (Media Release, 13 June 2017).

<sup>25</sup> Melanie Petrinec, ‘Former drug squad cop Peter Betts fined for misusing police computer system’, *Gold Coast Bulletin* (online), 14 March 2016.

<sup>26</sup> For other examples from Western Australia, see *Cogan v Velkovski* [2016] WASC 158; *Taylor v The State of Western Australia* [2015] WASCA 72; *Hull v The State of Western Australia* [2005] WASCA 194; *Casilli v Wehrmann* [2014] WASC 319; *Rhatigan v Forbes* [2009] WASC 368.



- in 2009 a former detective sergeant was given a 12 month suspended jail term after he pleaded guilty to 16 charges of unlawfully accessing the police system to obtain the details of women he was attracted to,<sup>27</sup> and
- as recounted in the case of *Inglis v Pinch*,<sup>28</sup> in 2016 a police officer was fined \$8,000 for accessing data about himself on the police system on three occasions, including information about his vehicle, and about two incidents in which he was the victim of an alleged crime.

[70] Case law in Western Australia has developed to the point where three factors are taken into account in weighing up the gravity of the offending. These factors are:

1. the nature of the information to which access was gained e.g. its personal sensitivity, or the potential public mischief stemming from access
2. the quantity of information the subject of the access, and
3. the purpose of the offender in gaining access.<sup>29</sup>

[71] In Victoria, a former VicRoads employee has recently pleaded guilty to several charges related to information access and use, including the equivalent legislation in section 247G of the *Crimes Act 1958* (Vic).<sup>30</sup> And in 2016 a civilian police employee pleaded guilty to eight offences under the New South Wales legislation.<sup>31</sup> The employee had used the database to access information about women known to her boyfriend.

[72] None of the above cases involved the public sector employee 'hacking' into the system, in the traditional sense of the word. Because of their jobs, they were authorised to access the systems and therefore did not need to 'hack'.

[73] It had been the Commission's understanding that unlike most, if not all, equivalent offences in other Australian jurisdictions, the Tasmanian unauthorised access offences would likely require 'hacking' in the traditional sense of the word.<sup>32</sup>

[74] However, the DPP has advised that in differing circumstances he would use various provisions of schedule 1 of the *Criminal Code Act 1924* (Tas) (*Criminal Code*) to prosecute. In a case in which a person improperly used a computer and some benefit or detriment arose from that use, he would be likely to charge under section 257B, dealing with computer-related fraud. He would also consider the use of section 253A, dealing with fraud more generally. He noted that this is a wide provision, the application of which would cover most public servants.

---

<sup>27</sup> 'Sex was cop's motive in accessing information, court told', *Australian Associated Press* (online), 17 November 2009; 'Disgraced cop escapes jail over computer hack', *Australian Associated Press* (online), 18 November 2009; 'Former police officer avoids jail over computer offence', *ABC News* (online), 18 November 2009.

<sup>28</sup> *Inglis v Pinch* [2016] WASC 30.

<sup>29</sup> *Inglis v Pinch* [2016] WASC 30, [36].

<sup>30</sup> Dan Oakes, 'Former VicRoads worker illegally supplied information from agency's database', *ABC News* (online), 5 March 2018.

<sup>31</sup> Richard Noone, 'Scorned woman uses cop database to harass lover', *The Daily Telegraph* (online), 21 December 2016; *Crimes Act 1900* (NSW) s 308H.

<sup>32</sup> The uncertainty of the law in Tasmania was noted in Australian Institute of Criminology, 'Hacking offences' (2005) 05 *High Tech Crime Brief*.

[75] Where no benefit or detriment arises, the relevant criminal offence is set out in s 257D. Titled 'Unauthorized access to a computer', there is a matching summary offence in section 43C of the *Police Offences Act 1935* (Tas).

[76] The Commission is not aware of any prosecutions of public sector employees under these offence provisions.

[77] In his submission on the draft of this report, the DPP advised that,

*a police officer or public servant only has authority to access a computer or part of a computer system pursuant to s 257D for work purposes. They have no authority to access it for a non-work purpose. Therefore, if they do it for a non-work purpose they have no lawful excuse and therefore they have committed an offence under s 257D of the Criminal Code.*

[78] The DPP agreed that 'there is uncertainty in respect to the interpretation and it would be useful to clarify that with legislation'.

### **Official corruption or bribery**

[79] Where information is shared in return for money or another benefit, bribery or corruption charges may be pursued. For example, in November 2017 a suspended Australian Federal Police (AFP) officer pleaded guilty to receiving a corrupting benefit. The officer had received about \$7,000 in return for information from a secure AFP database.<sup>33</sup>

[80] Bribery and corruption offences are 'notoriously difficult to prove ... [because benefits] ... may take many forms, not merely monetary, and are often difficult to discover'.<sup>34</sup> In Tasmania, it appears likely that such an offence would be even harder to make out than in other jurisdictions.

[81] The relevant offence – corruption of public officers – is set out in section 83 of the *Criminal Code*. The Commission is not aware of any recent prosecutions under this provision.<sup>35</sup> As the Commission has highlighted previously, the term 'public officer' in the *Criminal Code* is unlikely to apply to many public sector employees.<sup>36</sup> While finding that the commissioner of police is a 'public officer' under the *Criminal Code*, in *State of Tasmania v Johnston*, the Judge said that many, if not all, State Service employees are not public officers.<sup>37</sup> While he did outline his thoughts on State Service employees,

---

<sup>33</sup> Commonwealth Director of Public Prosecutions, 'Federal police officer gaoled for corruption' (Media Release, 22 November 2017).

<sup>34</sup> Criminal Justice Commission Queensland, *Protecting Confidential Information: A Report on the Improper Access to, and Release of, Confidential Information from the Police Computer Systems by Members of the Queensland Police Service* (November 2000) 107.

<sup>35</sup> There are two cases from the first half of the 20<sup>th</sup> century, see Integrity Commission, *Prosecuting serious misconduct in Tasmania: The missing link – Interjurisdictional review of the offence of 'misconduct in public office'* (October 2014) 41.

<sup>36</sup> Integrity Commission, *Prosecuting serious misconduct in Tasmania: The missing link – Interjurisdictional review of the offence of 'misconduct in public office'* (October 2014) 13.

<sup>37</sup> *State of Tasmania v Johnston* [2009] TASSC 60, [3], [62] (Evans J). Note that this means 'employee' as defined under s 3 of the *State Service Act 2000* (Tas). An 'officer' – as defined under s 3 of the *State Service Act 2000* (Tas) – would be a public officer under the *Criminal Code Act 1924* (Tas).

the Judge did not state which persons employed under the *PS Act* – other than the Police Commissioner – are public officers.

- [82] The Commission has previously recommended that the definition of ‘public officer’ in the *Criminal Code* be amended to align with modern standards, other Tasmanian legislation, and community expectations.<sup>38</sup> To date, this has not occurred.

### **Disclosure of official secrets**

- [83] Many jurisdictions have legislation that criminalises the disclosure of ‘official secrets’. As with corruption and bribery offences, these provisions are less commonly used. In Tasmania, the relevant provision is section 110 of the *Criminal Code*, which is as follows:

*Any public officer who discloses (except to some person to whom he is authorized to publish or communicate the same) any fact which comes to his knowledge, or the contents of any document which comes to his possession, by virtue of his office and which it is his duty to keep secret, is guilty of a crime.*

*Charge: Disclosing official secrets.*

- [79] As the offence must be committed by a ‘public officer’, in theory the same difficulties outlined above apply to this offence. However, the Commission is aware of a 2008 case in which a Tasmania Police officer pleaded guilty to the offence. The officer had accessed information about police operations and disclosed the information to their partner.<sup>39</sup>
- [80] This offence is also difficult to make out because it can be hard to prove that there was a duty not to disclose the information.<sup>40</sup> This was demonstrated in the relatively recent prosecution of the then commissioner of Police, Jack Johnston (*State of Tasmania v Johnston*). In that case, the Judge found that the police commissioner had ‘the authority to authorise disclosures that others might conclude were inappropriate’.<sup>41</sup> Because of his position, Mr Johnston had the authority to authorise the release of the information and the prosecution was permanently stayed.
- [81] It is the Commission’s view that section 110 of the *Criminal Code* would benefit from revision, and the DPP is of the same view. There are a number of elements of the offence which in practice are very difficult to prove. Apart from the issues relating to the definition of public officer, these practical difficulties revolve around the phrases ‘by virtue of his office’ and ‘duty to keep secret’. It is unnecessarily complex to prove what is a ‘duty’ of an office, as opposed to what may be incidental to that office.
- [82] In the Commission’s view, any new provision relating to disclosure of official secrets should encompass a broad definition of who is a public officer; should require the

---

<sup>38</sup> Integrity Commission, *Prosecuting serious misconduct in Tasmania: The missing link – Interjurisdictional review of the offence of ‘misconduct in public office* (October 2014) 44.

<sup>39</sup> *Tasmania v Tania Eirene Clarke*, 15 February 2008.

<sup>40</sup> For a brief discussion based on the Western Australian legislation, see LexisNexis, *Criminal Law WA* (at 16 April 2018) Chapter XII Disclosing official secrets [s 81].

<sup>41</sup> *State of Tasmania v Johnston* [2009] TASSC 60, [98] (Evans J).

improper disclosure of information to be established (i.e. there must be a mental element to the offence); and should not be limited to the use of a computer.

### **Misconduct in public office**

[84] In other Australian jurisdictions, along with computer hacking or unauthorised access to information, the most common charge for information abuse is 'misconduct in public office' (MIPO). MIPO 'refers to an abuse of power or misbehaviour while working in the public service'.<sup>42</sup>

[85] MIPO can be charged in addition to the specific offence:

*... the public interest is served in charging a police officer with the specific behaviour-relevant charge (for example, sexual assault or rape, trafficking in or possession of drugs, theft, bribery or extortion) and requiring the offender to face a charge that is directly related to the holding of public office and breach of behavioural expectations attached to that office. The offence of misconduct in public office arguably captures this element of the misconduct in a way that the more specific criminal charges do not.*<sup>43</sup>

[86] MIPO has been noted as an attractive option for prosecutors in the United Kingdom in relation to police officers that pass on confidential information from databases.<sup>44</sup> The court in the Victorian case of *R v Quach*<sup>45</sup> explained why MIPO could be used for abuse of information:

*[U]se of knowledge or information acquired by the office holder in the course of his or her duties for a private or other impermissible purpose may be inconsistent with the responsibilities of the office and calculated to injure the public interest. If the misuse of the information is of a serious nature and is likely to be viewed as a breach of the trust reposed in the office so as to bring the office into disrepute, the conduct will fall within the ambit of the offence whether or not it occurs in the course of public office.*<sup>46</sup>

[87] As the Commission has previously highlighted, Tasmania does not have a MIPO offence in its *Criminal Code*.<sup>47</sup> The Director of Public Prosecutions is of the opinion that other offences in the *Criminal Code* would capture MIPO conduct.<sup>48</sup>

[88] Examples of MIPO prosecutions from other jurisdictions are set out below.

---

<sup>42</sup> Victorian Ombudsman, *Investigation into the improper release of autopsy information by a Victorian Institute of Forensic Medicine employee Whistleblowers Protection Act 2001* (May 2011) 24.

<sup>43</sup> Cindy Davids and Marilyn McMahon, 'Police Misconduct as a Breach of Public Trust: The Offence of Misconduct in Public Office' (2014) 19(1) *Deakin Law Review* 89, 109.

<sup>44</sup> Cindy Davids and Marilyn McMahon, 'Police Misconduct as a Breach of Public Trust: The Offence of Misconduct in Public Office' (2014) 19(1) *Deakin Law Review* 89, 95–6.

<sup>45</sup> *R v Quach* [2010] VSCA 106.

<sup>46</sup> *R v Quach* [2010] VSCA 106 at [46] per Redlich JA (Ashley JA and Hansen AJA concurring), quoted in Ombudsman New South Wales, *Operation Prospect: Volume 6 Chapters 20-22 Access to and disclosure of confidential records* (December 2016) 786.

<sup>47</sup> Integrity Commission, *Prosecuting serious misconduct in Tasmania: The missing link – Interjurisdictional review of the offence of 'misconduct in public office'* (October 2014).

<sup>48</sup> William Cox, *Report of the Independent Reviewer* (May 2016) Independent Review of the Integrity Commission Act 2009, 95–99 [7.5].

## New South Wales

- [89] The case of *Hughes v R*<sup>49</sup> is an example of a police officer charged with MIPO in relation to access and use of information. Each of the two MIPO offences in that case involved both unauthorised access to and misuse of information. The Judge in the original case commented that:

*[t]he offences involved a gross breach of trust on [the police officer's] behalf. The community is entitled to have confidence in members of the Police Force and is entitled to expect that the confidential information held by police be used only for legitimate police purposes. Considerable weight must be placed on general deterrence when sentencing for such offences. ... In my view the objective seriousness of the misconduct of a holder of public office offences falls at the upper range of objective seriousness for offences of that kind.*<sup>50</sup>

- [90] In *Jansen v Regina*<sup>51</sup> a police officer had pleaded guilty to one count of MIPO for accessing sensitive information at the request of an external person and passing it on over a period of several weeks. Most recently, in 2018 an officer pleaded guilty to MIPO for accessing and passing on confidential information about an investigation into her partner.<sup>52</sup>

## Queensland

- [91] In June 2017, the Queensland CCC charged:

- a former sergeant with 44 counts of MIPO for accessing the police database without authorisation,<sup>53</sup> and
- an officer with nine unauthorised access offences and one MIPO offence after he accessed the police database ten times to 'undertake checks that were for a personal purpose and not for authorised work purposes'.<sup>54</sup>

- [92] In November 2016 the CCC charged an officer with one count of MIPO for running unauthorised searches on a police database and passing on confidential information.<sup>55</sup>

---

<sup>49</sup> *Hughes v R* [2014] NSWCCA 15.

<sup>50</sup> See Simpson CJ quoting Marien DCJ in *Hughes v R* [2014] NSWCCA 15, [42].

<sup>51</sup> *Jansen v Regina* [2013] NSWCCA 301.

<sup>52</sup> Sam Rigney, 'Police officer Donna Michelle Sharpe pleads guilty to hindering an investigation and perverting the course of justice over partner's boat theft', *The Advocate* (online), 2 March 2018.

<sup>53</sup> Crime and Corruption Commission Queensland, 'Former Brisbane police officer to appear in court for misusing confidential information - 28 June' (Media Release, 28 June 2017).

<sup>54</sup> Crime and Corruption Commission Queensland, 'CCC serves Brisbane policeman with a notice to appear in court for misusing database - 13 June' (Media Release, 13 June 2017).

<sup>55</sup> Crime and Corruption Commission Queensland, 'Central region police officer charged with criminal offences - 15 November 2016' (Media Release, 15 November 2016).

### *South Australia*

- [93] In South Australia, an officer who allegedly passed information to journalists has recently been found not guilty on seven MIPO charges; three remaining charges were dropped after the jury failed to reach a verdict.<sup>56</sup>
- [94] The case of *R v Austin*<sup>57</sup> was an unsuccessful appeal by a police officer following his conviction on ten counts of MIPO for giving information from a police database to his brother-in-law. His brother-in-law used the information in his employment at a debt collection and commercial investigation agency.

### *United Kingdom*

- [95] MIPO has also been used to charge public officers in the United Kingdom for misuse of information, including in some of the famous *News of the World* cases where public officers were selling information to journalists.<sup>58</sup>

### *Victoria*

- [96] The VicRoads worker mentioned above as having pleaded guilty to unauthorised access to information also pleaded guilty to MIPO.<sup>59</sup> Other Victorian cases include:
- *DPP v Marks*,<sup>60</sup> which was a sentencing appeal by a former constable who had pleaded guilty to one count of MIPO. The officer had provided criminal intelligence to a known drug dealer
  - *R v Quach*,<sup>61</sup> in which the officer had preyed on a vulnerable person he had met on duty, and
  - *R v Bunning*,<sup>62</sup> in which the officer had pleaded guilty to, among other things, ten counts of MIPO for giving information from police databases to a known drug dealer.

### **Offences created under police service legislation**

- [97] Establishing legislation for an organisation may also contain offences for abuse of information.

---

<sup>56</sup> *R v Martin* [2017] SADC 73; Rebecca Opie, 'Media leaks detective Peter Martin found not guilty of seven corruption charges', ABC News (online), 23 October 2017; Rebecca Opie, 'Prosecutors drop remaining corruption charges against SA detective accused of media leaks', ABC News (online), 24 November 2017.

<sup>57</sup> *R v Austin* [2013] SASCFC 133.

<sup>58</sup> *R v Chapman* [2015] QB 833

<sup>59</sup> Dan Oakes, 'Former VicRoads worker illegally supplied information from agency's database', ABC News (online), 5 March 2018.

<sup>60</sup> *DPP v Marks* [2005] VSCA 277.

<sup>61</sup> *R v Quach* [2010] VSCA 106.

<sup>62</sup> *R v Bunning* [2007] VSCA 205.

- [98] Legislation or regulations relating to the Australian Federal Police,<sup>63</sup> Northern Territory Police,<sup>64</sup> Queensland Police Service<sup>65</sup> and Victoria Police<sup>66</sup> all contain specific information-related offences for police officers. In South Australia, it appears that the only offence is in relation to former employees who use or disclose certain information.<sup>67</sup> In Western Australia, there does not appear to be any offence – although there are disciplinary offences.<sup>68</sup>
- [99] In Tasmania, there is no relevant offence, although there are specific sections of the Tasmania Police Code of Conduct relevant to the abuse of information.<sup>69</sup>
- [100] The case of *DPP v Zierk*<sup>70</sup> is an example of a failed attempt to prosecute a police officer under the Victorian legislation, for sending confidential police manuals to a former colleague. Examples of successful prosecutions under the Victorian legislation include:
- *D'Alo v Nolan*,<sup>71</sup> in which a police officer included confidential information in a published book, and
  - *DPP v Artz*,<sup>72</sup> in which a police officer gave information about a planned raid to a journalist.

### 3.4. Conclusion

- [101] There appear to be fewer options available for prosecuting public sector employees – including police officers – in Tasmania than in most Australian jurisdictions. At the very least, it seems unlikely that a public sector employee could be prosecuted for unauthorised access alone.
- [102] The Tasmania Police Professional Standards Commander told the Commission that if he was uncomfortable with the state of the law in Tasmania or if he felt that people were getting away with offences, then he would seek legislative change. His view was that, as things stood, he doesn't see that occurring.
- [103] Whether the current legislative scheme needs amendment is ultimately a decision for the Parliament of Tasmania. At a minimum, however, the Commission recommends that the Tasmanian offences for 'disclosure of official secrets' and 'computer hacking or unauthorised access to information' be reviewed.

<sup>63</sup> *Australian Federal Police Act 1979* (Cth) s 60A.

<sup>64</sup> *Police Administration Act* (NT) s 155.

<sup>65</sup> *Police Service Administration Act 1990* (Qld) ss 10.1, 10.2. As well as these general provisions, there are also specific provisions, such as about disclosures of criminal history and disciplinary information.

<sup>66</sup> *Victoria Police Act 2013* (Vic) ss 225–232 (which replaced *Police Regulation Act 1958* s 127A).

<sup>67</sup> *Police Regulations 2014* (SA) reg 93.

<sup>68</sup> *Police Force Regulations 1979* (WA) reg 607.

<sup>69</sup> The sections of the Code of Conduct most relevant to information are *Police Service Act 2003* (Tas) ss 42(4), (7), (8), (9) and (10).

<sup>70</sup> *DPP v Zierk* [2008] VSC 184.

<sup>71</sup> *D'Alo v Nolan* [2006] VSC 362.

<sup>72</sup> *DPP v Artz* [2013] VCC 56.

### **Recommendation no. 1**

It is recommended to the Premier that Tasmania's 'Disclosure of official secrets' and 'Unauthorized access to a computer' offences be reviewed, with a view to amending them to make the law more certain, and/or to align them with equivalent offences in other Australian jurisdictions.

The offences referred to are in sections 110 and 257D of schedule 1 of the *Criminal Code Act 1924* (Tas) and section 43C of the *Police Offences Act 1935* (Tas).



## 4. Policies and procedures on information management

---

- [104] There have been rapid advances in information technology over the last three decades. Thirty years ago, police officers did not have information at their fingertips, and if an officer needed information they had to request it from the relevant section.
- [105] Now, new recruits are reportedly often surprised by the amount of information held by Tasmania Police. Officers not only have direct access to that information while at work, they also have access from home on their police-issued computer tablets.
- [106] More ready access to more information, while undoubtedly increasing efficiency, also increases the risk of unauthorised access and misuse. Community expectations around information management have changed over time, as those risks have become more apparent.
- [107] It is important that public sector organisations have robust policies and procedures around information management. These should be under regular review to ensure that they reflect any changes in information technology and community expectations

### 4.1. Good practice

- [108] Policies and procedures on information access and use should be simple, clear<sup>73</sup> and accessible. This minimises the risk of misinterpretation.<sup>74</sup> Ideally, all relevant policies and procedures will be available in a single document – this can be achieved by, for example, the use of the organisation’s intranet.<sup>75</sup>

Public sector employees working with sensitive information should apply the ‘need to know’ principle.

- [109] The policies should be ‘aimed at increasing employees’ personal responsibility and focusing their minds on the importance of maintaining confidentiality’.<sup>76</sup> Organisations should not rely on an unstated and unwritten belief that employees are aware of the sensitivity of information and their responsibilities.<sup>77</sup>

This means that a person should only be made aware of something if they need to know the information in order to perform a job or role.

- [110] Where relevant, all public sector organisations’ policies and procedures should:

---

<sup>73</sup> Crime and Misconduct Commission Queensland, *Monitoring police ethics: a 2013 survey of Queensland recruits and First Year Constables* (October 2013) Research and Issues Paper Number 13, 1.

<sup>74</sup> Office of Police Integrity Victoria, *Sensitive and confidential information in a police environment: Discussion paper no.2* (June 2010) 22.

<sup>75</sup> Office of Police Integrity Victoria, *Sensitive and confidential information in a police environment: Discussion paper no.2* (June 2010) 22; Julie People, ‘Research and Issues Papers Number 02: Unauthorised Disclosure of Confidential Information by NSW Police Officers’ (October 2008) *Police Integrity Commission New South Wales* 28.

<sup>76</sup> Australian Securities & Investments Commission, *Consultation Paper 128: Handling confidential information* (December 2009) 16.

<sup>77</sup> Australian Securities & Investments Commission, *Consultation Paper 128: Handling confidential information* (December 2009) 16.

- discuss the risks
- cover use, modification, handling and storage of electronic and hardcopy information
- cover authorisations and processes for the release of information
- be consistent in the use of, and define, key terms such as 'confidential information'
- provide guidance on what to do if approached for information
- make it clear that the organisation audits access, and takes action when unauthorised accesses are identified
- include the possible penalties for abuse of information and links to disciplinary policies and procedures, and
- clarify that providing any information without authorisation is a leak, regardless of to whom it was given and whether or not there were tangible benefits.<sup>78</sup>

[111] Governance steps that can be taken by public sector organisations include:

- assigning responsibility for information management to one body or individual,<sup>79</sup> and
- incorporating confidential information in internal audit and corruption risk management processes.<sup>80</sup>

### **Policy specifics for police services**

[112] Police policies and procedures should specifically identify that it is not appropriate to use a work database to look up records such as the below:

- of a person with whom they are wishing to associate or are considering a relationship
- of an associate, friend or relative where involvement with the police is suspected
- of an individual who has been mentioned to them and about whom they are curious
- of an individual who is about to be employed by a friend or relative

---

<sup>78</sup> Crime and Corruption Commission Queensland, *Corruption Prevention Advisory: Information security and handling* (September 2016) 2; Crime and Corruption Commission Queensland, *Corruption Prevention Advisory: Use of official resources* (July 2017) 6; Independent Commission Against Corruption New South Wales, *Confidential information* (Undated) Preventing Corruption <[www.icac.nsw.gov.au/preventing-corruption/known-your-risks/confidential-information/4913](http://www.icac.nsw.gov.au/preventing-corruption/known-your-risks/confidential-information/4913)>; Office of Police Integrity Victoria, *Investigation into Victoria Police's Management of the Law Enforcement Assistance Program (LEAP)* (March 2005) 33; Australian Commission for Law Enforcement Integrity, *ACLEI Top 5 Corruption Prevention Myths* (Undated) <[www.aclei.gov.au/corruption-prevention/corruption-prevention-myths](http://www.aclei.gov.au/corruption-prevention/corruption-prevention-myths)>; Office of Police Integrity Victoria, *Sensitive and confidential information in a police environment: Discussion paper no.2* (June 2010) 20, 22; Julie People, 'Research and Issues Papers Number 02: Unauthorised Disclosure of Confidential Information by NSW Police Officers' (October 2008) *Police Integrity Commission New South Wales* 29.

<sup>79</sup> Office of the Australian Information Commissioner, *Guide to information security* (April 2013) 16.

<sup>80</sup> Independent Commission Against Corruption New South Wales, *Confidential information* (Undated) Preventing Corruption <[www.icac.nsw.gov.au/preventing-corruption/known-your-risks/confidential-information/4913](http://www.icac.nsw.gov.au/preventing-corruption/known-your-risks/confidential-information/4913)>.

- to check a vehicle before buying it
- of prospective neighbours to see if they have links to criminals
- as a part of a self-training exercise, or
- relating to themselves.<sup>81</sup>

[113] On first glance, it can be hard to explain why some of the above are not authorised accesses undertaken for legitimate work purposes. When one considers the sensitive nature of the information held on police databases, it becomes more obvious why such accesses are not generally appropriate.

[114] This quote from the New South Wales Ombudsman also helps to illustrate the point:

*The Senior Constable is mistaken in his belief that he can access his own details at will. Authority to access any specific information rests with the Police Service, not with the person whose details are stored therein. An officer has no more right to check information contained within the system concerning himself than any member of the public has to look up his own criminal history or any criminal has to check what information is stored in the Police Service intelligence database concerning his illegal activities.*<sup>82</sup>

[115] The case of *Inglis v Pinch*<sup>83</sup> is an example of a West Australian police officer who was prosecuted for accessing his own records on a police database. An apparently innocent viewing of records about oneself can also lead to other infractions (the ‘slippery slope’).

## 4.2. Other jurisdictions

[116] This investigation did not include a detailed survey of policies and procedures in other police jurisdictions, nor were records requested directly from other Australian police services. Some good practice material from other jurisdictions was located through open source research and is outlined below.

### **Australian Federal Police (AFP)**

[117] The AFP has a national guideline on information management.<sup>84</sup> The guideline emphasises the importance of data integrity and the need for a ‘single source of truth’. It states that the need to share principle is a ‘fundamental premise’ of the AFP.

[118] The guideline outlines the AFP’s information security principles of: clear desk, need to know, access management, risk management, and information handling. The AFP has

---

<sup>81</sup> Criminal Justice Commission Queensland, *Protecting Confidential Information: A Report on the Improper Access to, and Release of, Confidential Information from the Police Computer Systems by Members of the Queensland Police Service* (November 2000) 57.

<sup>82</sup> Office of the NSW Ombudsman, quoted in Criminal Justice Commission Queensland, *Protecting Confidential Information: A Report on the Improper Access to, and Release of, Confidential Information from the Police Computer Systems by Members of the Queensland Police Service* (November 2000) 57–8.

<sup>83</sup> *Inglis v Pinch* [2016] WASC 30.

<sup>84</sup> Australian Federal Police, *AFP National Guideline on information management* (Undated) <[www.afp.gov.au/about-us/information-publication-scheme](http://www.afp.gov.au/about-us/information-publication-scheme)>.

‘information stewards’ who are the ‘information management champions in their work places’.

### **New South Wales Police Force (NSWPF)**

[119] The NSWPF has a privacy management plan that states:

*It is therefore critical to community confidence for people to know that we will handle information lawfully and in a way that strikes the right balance between an individual's privacy and the community's safety.*<sup>85</sup>

[120] The plan explains how the NSWPF complies with privacy and health records legislation. It contains examples of NSWPF training, and data retention and security measures.

### **New Zealand Police**

[121] The New Zealand Police Code of Conduct places particular emphasis on the security of information,<sup>86</sup> and classifies ‘unauthorised access to, or disclosure of any matter or information related to Police business including [the police database NIA]’ as serious misconduct.<sup>87</sup> Under the heading ‘our information’, it states:

*Given the nature of our organisation and information systems, we have access to confidential, sensitive and personal information. As Police we are trusted by those we serve to be exemplary in our dealings with this information. We need to consistently practice good judgement and integrity when creating, accessing, modifying and using, securing and disclosing all information. We always need to handle information appropriately, for legitimate work purposes and in line with the law, our policies, processes and systems.*

*When we are unsure whether information is confidential or sensitive or how it should be handled, we seek advice from our manager.*<sup>88</sup>

### **Queensland Police Service (QPS)**

[122] The QPS *Management Support Manual* contains detailed processes for the release of different kinds of information, such as criminal histories.<sup>89</sup>

---

<sup>85</sup> New South Wales Police Force, *Privacy Management Plan* (2013) 1 <[www.police.nsw.gov.au/about\\_us/policies\\_procedures\\_and\\_legislation](http://www.police.nsw.gov.au/about_us/policies_procedures_and_legislation)>.

<sup>86</sup> Laura Tidey, ‘Rogers v Television New Zealand Ltd: Police and the Release of Information to the Media’ (2009) 40 *Victoria University of Wellington Law Review* 507, 515.

<sup>87</sup> New Zealand Police, *Our Code* (2015) 8 <[www.police.govt.nz/about-us/publication/new-zealand-police-code-conduct](http://www.police.govt.nz/about-us/publication/new-zealand-police-code-conduct)>.

<sup>88</sup> New Zealand Police, *Our Code* (2015) 5 <[www.police.govt.nz/about-us/publication/new-zealand-police-code-conduct](http://www.police.govt.nz/about-us/publication/new-zealand-police-code-conduct)>.

<sup>89</sup> Queensland Police Service, *Chapter 5: Information Management and Privacy* (29 March 2018) Management Support Manual <[www.police.qld.gov.au/corporatedocs/OperationalPolicies/msm.htm](http://www.police.qld.gov.au/corporatedocs/OperationalPolicies/msm.htm)>.

## United Kingdom

- [123] In the United Kingdom, there is a *Code of Practice on the Management of Police Information*, which is a statutorily sanctioned document issued by the Secretary of State for the Home Department.<sup>90</sup> More detailed guidance is found in the online resource about police information management hosted by the College of Policing.<sup>91</sup>

## Western Australia Police (WAPOL)

- [124] The WAPOL Code of Conduct contains a section titled ‘access to WA Police information holdings’. The content of that section is reproduced below in full, as it effectively covers off on much of the content of good practice policies as outline above (emphasis in original).

*The management, access and use of information stored on police computer systems are areas of growing concern. It represents a considerable and very real risk to both the employee and the organisation if the appropriate rules and protocols are not observed.*

*Being a police officer or police staff member does not give you “licence” to search or surf through police records which are not strictly related to your work duties, authorisation, role or function. Your access to WA Police information holdings is limited to specific information that has a direct relationship to your work area or associated work functions.*

*Access to information that relates solely to a user’s personal, private, business or social interests is prohibited. This also includes for reasons solely related to protecting a user’s reputation as a member of the WA Police. **Where any doubt exists, authority should be obtained from a direct supervisor. Do not risk the consequences of acting inappropriately.***

*Employees are not to leave computers open and unattended once access has been obtained. Individuals will be held personally accountable if they offer such conduct as an explanation when information access is in question. Section 440A of the Criminal Code (Unlawful Use of Computers) does not require ‘the gaining of a benefit’ or the ‘causing of a detriment’ for an employee to be guilty of a criminal offence under this section.*

*To simply ‘use’ the computer when ‘not properly authorised’ or ‘otherwise than in accordance with his or her authorisation’ means the person may be committing a serious offence under the Criminal Code.<sup>92</sup>*

- [125] Other relevant sections of the WAPOL Code of Conduct include inappropriate communication and confidentiality.<sup>93</sup>

---

<sup>90</sup> Secretary of State for the Home Department/National Centre for Policing Excellence, *Code of Practice on the Management of Police Information* (July 2005) <[library.college.police.uk/docs/APPref/Management-of-Police-Information.pdf](http://library.college.police.uk/docs/APPref/Management-of-Police-Information.pdf)>.

<sup>91</sup> College of Policing, *Information management* (23 October 2013) Authorised Professional Practice <[www.app.college.police.uk/app-content/information-management/](http://www.app.college.police.uk/app-content/information-management/)>.

<sup>92</sup> Western Australia Police, *Code of Conduct* (August 2010) 11–12.

<sup>93</sup> Western Australia Police, *Code of Conduct* (August 2010) 12–13, 17.

### 4.3. Tasmania Police

- [126] In 2005, Tasmania Police took its first readily apparent steps toward introducing and enforcing stricter and more broad-ranging policies and procedures around access to and use of information. The centerpiece was a notice issued by the then police commissioner, Richard McCreadie. Officers spoken to as part of this investigation were unsure what instigated these steps, but the commissioner's notice does say that there had been an increase in complaints.
- [127] In unequivocal terms, the notice stated that access to information must be for work related purposes only, that audits will be undertaken, and that adverse findings could result in 'serious sanctions including termination of employment'. The notice outlined a number of strategies that would be used to clarify expectations.
- [128] Tasmania Police policies and procedures have changed since 2005. The current framework is outlined below.

#### Code of Conduct

- [129] The overarching obligations for Tasmania Police officers on information access and use are set out in the Code of Conduct, which is in section 42 of the *PS Act*. Although any section of the Code could be relevant to abuse of information (depending on the situation), five of the 13 sections are more directly relevant.

##### **42. Code of conduct**

...

*(4) A police officer must maintain appropriate confidentiality about any dealing made and information gained in the course of his or her duties in the Police Service.*

...

*(7) A police officer, in connection with his or her duties in the Police Service, must not –*

*(a) knowingly provide false or misleading information; or*

*(b) omit to provide any matter knowing that without that matter the information is misleading.*

*(8) A police officer must not make improper use of –*

*(a) information gained in the course of his or her duties in the Police Service; or*

...

*in order to gain, or seek to gain, a gift, benefit or advantage for the police officer or for any other person.*

*(9) A police officer must not access any information to which the police officer is not entitled to have access.*

*(10) A police officer must not destroy, damage, alter or erase any official document, record or entry without the approval of the Commissioner.*

...

## Tasmania Police Manual

[130] Under section 93 of the *PS Act*, the Police Commissioner must publish the 'Police Manual'. The Tasmania Police Manual (TPM) is the rule book for police officers. Most of the TPM amounts to guidance, although it also contains Police Commissioner 'orders'. Failure to follow an order is a breach of the Code of Conduct.<sup>94</sup>

[131] The parts of the TPM most relevant to information access and use are set out below:

- Part 11 – Correspondence and communication

This part covers how to write, protect and process documents, including assigning security classifications. It includes an order stating that officers 'shall not supply or disclose any police file or portion thereof to any person outside the Department unless authorised by the Commissioner'. Under the classified documents section, it states that access to documents should normally be on a need to know basis, and that access just because of rank or status should not be permitted.

- Part 12 – Information and communications management

This part briefly covers records management and archiving, and refers officers to a policy document for more detailed guidance. It has more detailed instructions on authorisations and processes for the release of information, as well as radio and telephone communications.

- Clause 13.2.2 – Access, disclosure and supply of information

Contained within Part 13, which is about misconduct and complaints against police, clause 13.2.2 is newly drafted. The clause has been written in light of learnings from the recent round of Tasmania Police audits (see below). It is simply and clearly drafted. It includes an order about access to and use of information, and prohibits officers from accessing their own information, accessing information to satisfy personal interest or simple curiosity, and accessing information relating to persons they know unless 'there is a reason directly related to their work duties and they have express permission' from an officer of rank inspector or above.

[132] Meetings with senior police and the audits currently being undertaken by Tasmania Police indicate that there have been 'grey areas' for officers in terms of access to information. This has informed the drafting of the new TPM clause.

[133] The audits have revealed that, while some officers were clear on their responsibilities, others were not so clear. There has been some difference of opinion even among senior officers. Examples of these grey areas include:

- running checks on a new acquaintance to ensure they are not linked to criminals
- performing a self-training exercise or broadening knowledge about future work areas e.g. drug crime
- accessing details about their own vehicle or licence – including when required for work purposes, for instance to fill out a training form, and

---

<sup>94</sup> *Police Service Act 2003* (Tas) s 42(3)(a).

looking up colleagues to match a face to the name or voice.

### **Other policies and procedures**

[134] Other relevant Tasmania Police policies and procedures include:

- a booklet titled *Information Systems Access Control Guidelines*
- *Department of Police and Emergency Management Policy Document No. 01/14 Employee Directions for the use of Mobile Computing Devices*
- *Department of Police and Emergency Management Acceptable Use Policy – Internet and Email* (November 2008),
- *Information Security Policy*, and
- *Department of Police and Emergency Management TRIM Procedures and Guidelines*.<sup>95</sup>

[135] In accordance with the *Information Security Policy*, Tasmania Police has an Information Security Committee and an Information Security Unit. The responsibilities of these bodies include providing advice on information security and auditing compliance with information security policies and guidelines.

### **Conduct and complaints management system**

[136] In March 2018, Tasmania Police implemented a new conduct and complaints management system, *Abacus – Commissioner’s Directions for Conduct and Complaint Management, and Compliance Review*. *Abacus* was developed by police in response to a review (undertaken jointly by police and the Commission) of the previous Graduated Management Model.

[137] *Abacus* is a centralised reference document that brings together all of the information relevant to the management of conduct, complaints, and compliance matters. It is established under section 43(1) of the *PS Act* as a procedure for the investigation into any alleged breach of a provision of the Code of Conduct by a police officer. Its focus is – except in more serious offences – on professional development.

[138] *Abacus* applies to police officers but not to state service employees of the Department of Police, Fire and Emergency Management. It is publicly available to ensure transparency and clarity for both members and the public. It will be amended as required to ensure the information is contemporary.

## **4.4. Conclusion**

[139] The Commission considers that, generally, Tasmania Police policies and procedures on information management meet good practice standards.

---

<sup>95</sup> ‘TRIM’ is one of several databases used by Tasmania Police.



[140] In particular, the new clause 13.2.2 of the TPM effectively covers off on many of the features of good practice policy outlined above. Hopefully, the clause will resolve many of the 'grey areas' in terms of information access.

[141] Also, the introduction of the new conduct and complaints management system – *Abacus* – will ensure a focus on continuing professional development with the aim of improving police conduct and performance. *Abacus* provides an efficient mechanism for linking the Code of Conduct with the TPM sections, and policies and procedures relevant to information management in one document, available internally and to the general public. It is a system which could be used as a basis for misconduct and complaint management systems developed by other public sector agencies.

[142] Areas in which the Commission considers that Tasmania Police policies and procedures could be improved include by:

- placing more emphasis on the need to know principle, and
- making it clear in TPM clause 13.2.2 that:
  - providing any information without authorisation is a leak, regardless of to whom it was given and whether or not there were tangible benefits
  - officers must not should not run searches on 'suspect' individuals, even if they perceive that as necessary to protect their reputation as a police officer (for instance if they suspect a new acquaintance has links to criminals)<sup>96</sup>
  - audits are being undertaken, and
  - appropriate action will be taken when unauthorised access or misuse is identified.

---

<sup>96</sup> As discussed earlier, this has been a grey area for Tasmania Police in the past.

## 5. Information security policies, practices and procedures

---

[143] With technological advances being made every day, good information security is important to protect data from both external and internal threats. Information is valuable, and in the wrong hands it can be spread far and wide at the press of a button.

### 5.1. Good practice

[144] Information security controls should minimise or eliminate the excuses available to avoid accountability for unauthorised access or misuse.<sup>97</sup>

[145] Some key aspects of good information security include:

- an ability and willingness to audit employee access to information
- only providing access to those who genuinely need to have access, including by removing access rights from employees who are, for example, on long term leave or stood down
- adequate training on systems usage
- undertaking risk and privacy impact assessments, especially when introducing new policies
- regular monitoring and review of the relevance and effectiveness of security measures that protect personal or sensitive information
- requiring employees to sign an acknowledgement that they understand their responsibilities in regard to information – if an employee is accused of information abuse, the acknowledgement can be used to show that they were aware of their responsibilities
- a requirement to assign a security classification to an email before sending it
- alert monitoring of selected records and transactions on databases, and

---

<sup>97</sup> Office of Police Integrity Victoria, *Investigation into Victoria Police's Management of the Law Enforcement Assistance Program (LEAP)* (March 2005) 23.

- requiring users of restricted databases to enter passwords, agree to an acknowledgement of use on login, and enter 'reasons for access' (RFA).<sup>98</sup>

[146] Entering an RFA is a required part of accessing some restricted systems. A recorded RFA is important both in terms of personal and organisational accountability. Employees should be held accountable if they submit a nonsense RFA and later claim that they cannot recall their reason for the access. Examples of poor RFAs include entering 'w' (for 'work') and 'enq' (for 'enquiry').

[147] Police organisations should also consider analysing internet and email usage to detect suspicious patterns.<sup>99</sup> This may include behaviour such as 'continuing to text or phone victims of crime or offenders following initial contact, being overly friendly and familiar, displaying an unusual interest in or preference for attending a particular type of incident or dealing with those in a vulnerable position'.<sup>100</sup>

[148] Employees should also be made aware of simple steps they can take to maintain information security, such as locking their computer when away from their desk, maintaining a 'clean desk' policy, and logging out of databases or turning off computers when not in use.

## 5.2. Tasmania Police

[149] Tasmania Police uses many of the good practice information security measures listed above. In particular, it:

- has an ability and willingness to audit access to information
- requires employees to sign an acknowledgement that they understand their responsibilities – recruits must sign a basic acknowledgement on their first night in the Police Academy

<sup>98</sup> David Smith and Tim Lee, 'When there is a breach – Know your obligations and what steps to take' (2015) 88 *Computers & Law* 1, 6; Australian Securities & Investments Commission, *Consultation Paper 128: Handling confidential information* (December 2009) 31; Office of the Australian Information Commissioner, *Guide to information security* (April 2013) 1; Crime and Corruption Commission Queensland, *Corruption Prevention Advisory: Information security and handling* (September 2016) 4; Office of Police Integrity Victoria, *Sensitive and confidential information in a police environment: Discussion paper no.2* (June 2010) 25; Independent Broad-based Anti-Corruption Commission, *Predatory behaviour by Victoria Police officers against vulnerable persons: Intelligence report 2* (December 2015) 9; Criminal Justice Commission Queensland, *Protecting Confidential Information: A Report on the Improper Access to, and Release of, Confidential Information from the Police Computer Systems by Members of the Queensland Police Service* (November 2000) 49–50, 64, 74; Independent Commission Against Corruption New South Wales, *IT systems* (Undated) Preventing Corruption <[www.icac.nsw.gov.au/preventing-corruption/knowning-your-risks/it-systems/4911](http://www.icac.nsw.gov.au/preventing-corruption/knowning-your-risks/it-systems/4911)>; Office of Police Integrity Victoria, *Investigation into Victoria Police's Management of the Law Enforcement Assistance Program (LEAP)* (March 2005) 27; Crime and Corruption Commission Queensland, *Confidential information: Unauthorised access, disclosure and the risks of corruption in the Queensland public sector* (May 2016) 5; Australian Commission for Law Enforcement Integrity, *Investigation Report: An investigation into the conduct of an Australian Federal Police appointee in relation to unauthorised disclosure of information and the giving of testimonials* (Report 03/2012) (17 October 2012) 4; Independent Commission Against Corruption New South Wales, *Confidential information* (Undated) Preventing Corruption <[www.icac.nsw.gov.au/preventing-corruption/knowning-your-risks/confidential-information/4913](http://www.icac.nsw.gov.au/preventing-corruption/knowning-your-risks/confidential-information/4913)>.

<sup>99</sup> Crime and Corruption Commission Queensland, *Corruption Prevention Advisory: Information security and handling* (September 2016) 4.

<sup>100</sup> Independent Police Complaints Commission, *The abuse of police powers to perpetrate sexual violence* (September 2012) 9.

- requires users of restricted databases to enter passwords and agree to an acknowledgement of use on login, and
- performs alert monitoring of selected records and transactions on databases.

[150] However, it did seem apparent from the Commission's audit of files that officers are not automatically logged out of one of the main police databases (IDM). This means that, in theory, they can (unknowingly) be logged in for days. Additionally, one officer did not realise that they could log out of one of the other police databases (ICE).

### **Alert monitoring**

[151] Integrity Commission audits indicate that Tasmania Police routinely puts 'flags' (alert monitoring) on prominent database entities. For example, if a famous Tasmanian is charged with a criminal offence, a flag is set up on the relevant database entries. These flags trigger an alert to Professional Standards when accessed by an employee. Checks are then done to see if the access was authorised.

### **Reasons for access**

[152] A number of Tasmania Police databases require the user to enter a RFA. Like other police services, Tasmania Police has had difficulty communicating the importance of the RFA process to its employees. It is now trying to raise awareness about the importance of RFAs as part of recruit training and through its audits. As explained below, audited employees are told in a formal letter if their RFAs could be improved.

### **Police-issued mobile computing devices (tablets)**

[153] Many Tasmania Police officers have a personal work-issued tablet that they may use as they see fit, including by taking it home. From the tablet, they can access a range of police databases. There are obvious risks involved in this, including the inadvertent disclosure of information by forgetting to lock the tablet.

[154] The organisation has a policy on the use of the tablets that acknowledges and intends to mitigate these risks. The tablets are password protected. The Commission was told that officers are not allowed to let other people use them, although that is not specified in the policy. The policy does state several times that the tablets may be audited, including remotely. It also states that officers are responsible for ensuring that 'any departmental systems including the police intranet is not accessed or viewed' by persons not employed by the Department.

### **Removing and restricting access rights**

[155] It is not common practice for Tasmania Police to restrict its officers' access rights. This includes officers that have been suspended or are under investigation for abuse of information, and officers that are on long term leave. Access restrictions have been imposed in very rare cases, for example when there is a public safety risk.

[156] The reason for Tasmania Police's reluctance to restrict access and/or restrict potential for communication with colleagues is because:

- even when an employee is suspended for alleged information abuse, the allegation is still unproven
- in nearly all cases, officers need access to information to do their job – if access were to be restricted, in many cases they would need to be reallocated or stood down even when this is otherwise unnecessary, and
- Tasmania Police wants its officers to feel part of the organisation, even when on long-term leave, and so encourages them to maintain their communications with the organisation.

[157] One of the files audited by the Commission as part of this investigation involved the alleged leaking of information by a disgruntled officer on long-term leave. Tasmania Police's assessment of this allegation was that it was unproven. However, the Commission considered that – on the balance of probabilities – the officer did access and leak the information. Had the officer's access rights been restricted, the information would not have been leaked. During the investigation, Tasmania Police advised that it is unrealistic to sever an officer's access to his workplace whilst on leave, as the allegation remained under investigation, and in any event, the matter at hand did not warrant suspension of the officer (which is when station access and IT access – by tablet removal – would be denied. Further, the finalisation of this particular matter occurred after the officer was no longer a member of Tasmania Police, and therefore the Code of Conduct could not apply to the officer, in so far as the application of sanctions under the *PS Act*.

#### ***Access to information awareness plan and system audits***

In December 2016, the Tasmania Police executive approved the '*Access to Information Awareness Plan*'. This was shortly after the Commission discussed information abuse with the then Professional Standards commander as part of its annual audit process.

One key aspect of the plan was to remind employees of their responsibilities through the *Tasmania Police Gazette*, the intranet and posters. The most substantive part of the plan was to commence a proactive audit program of police officer access to databases. In the past, audits had only been undertaken on a reactive basis, for example when a complaint was received. A pilot audit program was run in July 2017.

The audit program is currently ongoing. Tasmania Police aims to audit about 50 randomly selected police officers per month, meaning that every officer – up to and including the Commissioner – would get audited once every two years. The same program has also been initiated for State Service employees working in Tasmania Police.

The audits involve a general check of each officer's access over the preceding month. If any issues are detected, a more in-depth search of the officer's accesses is undertaken. A check is also performed to see if any other officer is accessing information about that officer.

Audits are also undertaken on accesses to information about prominent persons.

Each officer audited receives one of three possible letters, which state that they have been audited and:

no issues were detected

no access issues were detected, but their 'reasons for access' could be improved, or

they need to explain some of their accesses.

Between July 2017 and early April 2018, Tasmania Police audited 338 officers (both randomly as part of the program and targeted). Of those audits, 72 led to further inquiry or investigation. This usually included, as a first step, asking the officer to explain their access.

At the time of writing, 26 of the 338 officers audited were found to have breached the Code of Conduct for unauthorised access to information. Twelve of the matters subject to further inquiry or investigation are outstanding. Tasmania Police reports that the most common unauthorised accesses were to another officer's data, with some officers accessing information about family or friends.

Although the system audits have identified that there is room for improvement in terms of access to information, they have not found misuse (or unauthorised disclosure) of information to be a problem.

Due to word about the audits spreading throughout the organisation, the officers undertaking the audits have already identified a drop in the percentage of unauthorised accesses.

### 5.3. Conclusion

[158] It appears to the Commission that Tasmania Police is meeting many of the good practice information security requirements.

[159] In particular, Tasmania Police is to be commended for its proactive audit program. The Commission considers that this sets a good example for other Tasmanian public sector organisations that hold sensitive information.

[160] The Commission does think that the current program may be too resource intensive to maintain. As long as a representative sample of officers continue to be randomly selected, there seems to be no need to cycle through the entire organisation every two years.

[161] It is noted that the assigning of a security classification before sending an email is not required by Tasmania Police. However, as far as the Commission is aware, this measure is not currently used by any Tasmanian public sector organisation (including the Commission).

[162] In regard to warnings given when accessing restricted databases, the wording used by Tasmania Police is simple and clear. However, there is possibly room for improvement in the training of officers on database use.

[163] The Commission considers that the acknowledgement of responsibilities process could be improved. First, the wording should be expanded. For example, it should more

clearly outline the importance and sensitivity of information, and the ramifications if officers abuse information. The wording could be modelled on TPM clause 13.2.2.

[164] Second, the acknowledgment should be signed at the end of recruit training or when officers first become operational – this is when they will have a better understanding of what they are signing. As recruits do use databases during training, it may be necessary for them sign the acknowledgement at the start of their training as well (as they currently do).

[165] Finally, access restrictions should be more proactively considered by Tasmania Police. This is particularly the case where an employee has been suspended, stood down or is on long-term leave – especially if they are subject to allegations of information abuse.

[166] While the Commission understands Tasmania Police reluctance to restrict access rights, in some cases this will not outweigh the risk to private and sensitive information that the employee may pose. Where information access is not so integral to an employee's day-to-day work, information access restrictions should be even more proactively considered.

## 6. Culture and training

---

### 6.1. Good practice

[167] Police officers are, by nature, curious: it's part of why they are employed to do what they do, and part of what makes them good at what they do. This organisational trait can be antithetical to protecting information from unauthorised access.

[168] This means that, as outlined above, the rules (i.e. policies and procedures) need to be simple and clear. The organisation also must educate its employees about those rules. And it is important for managers, supervisors and the executive to model good behaviour and policy compliance.<sup>101</sup> Policies and procedures are all but irrelevant if employees are unaware of them, or if organisational culture is poor.

[169] Given the importance of information and curiosity to the average police officer's work, it is important to get the balance right between instilling a 'need to know' culture and allowing police enough scope to achieve the objectives of their work. According to the former Victorian Office of Police Integrity, this can be achieved

*in a positive manner ... by reinforcing the principles through messages that emphasise that:*

- *it is not that the organisation does not trust employees – it is because information-seekers can use practices that can trip up even the most experienced employee; or*
- *if an officer does not know, the officer cannot tell.*<sup>102</sup>

[170] Officers should be educated about their 'vulnerability ... as targets for information-seekers', and should 'understand that they too possess the same susceptibilities as all humans'.<sup>103</sup>

[171] In terms of building a good organisational culture, it is also important to select the right people in the first place. Police organisations should have stringent control measures in place to ensure they are only employing persons suited to the job.

### 6.2. Other jurisdictions

[172] As previously mentioned, the Commission had intended to survey Tasmania Police officers as part of this investigation. The survey would have provided a better understanding of police culture on information access and use. Although the

---

<sup>101</sup> Independent Commission Against Corruption New South Wales, *Tip sheet for employees: Use and misuse of public sector resources* (February 2008) 4; Australian Commission for Law Enforcement Integrity, *ACLEI Top 5 Corruption Prevention Myths* (Undated) 2 <[www.aclei.gov.au/corruption-prevention/corruption-prevention-myths](http://www.aclei.gov.au/corruption-prevention/corruption-prevention-myths)>; Office of Police Integrity Victoria, *Information Security and the Victoria Police State Surveillance Unit* (February 2010) 38; Office of Police Integrity Victoria, *Sensitive and confidential information in a police environment: Discussion paper no.2* (June 2010) 20.

<sup>102</sup> Office of Police Integrity Victoria, *Sensitive and confidential information in a police environment: Discussion paper no.2* (June 2010) 28.

<sup>103</sup> Office of Police Integrity Victoria, *Sensitive and confidential information in a police environment: Discussion paper no.2* (June 2010) 20; Australian Commission for Law Enforcement Integrity, *ACLEI Top 5 Corruption Prevention Myths* (Undated) 2 <[www.aclei.gov.au/corruption-prevention/corruption-prevention-myths](http://www.aclei.gov.au/corruption-prevention/corruption-prevention-myths)>.



Commission was unable to run the survey, similar surveys have been conducted in other Australian jurisdictions.

[173] In Queensland, a 2013 survey of police recruits and first year constables indicated that at least new police officers take information access and use seriously:

- of a variety of types of wrongdoing presented, respondents rated sharing confidential police information with an unauthorised person and lying in a police report as two of three most serious types of behaviours
- lying in a police report was considered the most serious behaviour, and
- almost all respondents were most inclined to report another officer who shared confidential police information with an unauthorised person or lied in a police report.<sup>104</sup>

[174] This is hopefully reflective of a change in that police service, as a 2000 report had found some concerning cultural issues:

- officers seemed to apply a 'subjective test as to whether they should provide the information [to an unauthorised person] rather than abiding by the law and QPS policies'
- there was 'an unwillingness by many officers to accept that the release of a citizen's private details is wrong and potentially harmful', and 'where their entrenched view conflicted with the law, it was their view that prevailed', and
- suspect officers hid behind claims that they could not recall why they performed a search, that they could have performed it for someone else, or that they may have left their computer terminal open and someone else used their login.<sup>105</sup>

[175] A recent survey of Victoria Police officers seemed to demonstrate that many officers in that state had a good understanding of what amounted to misconduct and/or corruption, including:

- disclosing confidential information to unauthorised members of the community
- a police officer repeatedly asking a victim out on a date, and
- a police officer passing confidential information to a friend.<sup>106</sup>

### **6.3. Tasmania Police**

[176] As it was unable to run a survey, the Commission does not have a complete picture of Tasmania Police culture and training in regard to information access and use.

[177] Anecdotal reports from recruits and a meeting with a Police Academy officer indicate that, in Tasmania, the seriousness of unauthorised access to and misuse of

---

<sup>104</sup> Crime and Misconduct Commission Queensland, *Monitoring police ethics: a 2013 survey of Queensland recruits and First Year Constables* (October 2013) Research and Issues Paper Number 13, 1, 4–5.

<sup>105</sup> Criminal Justice Commission Queensland, *Protecting Confidential Information: A Report on the Improper Access to, and Release of, Confidential Information from the Police Computer Systems by Members of the Queensland Police Service* (November 2000) 18, 28.

<sup>106</sup> Independent Broad-based Anti-Corruption Commission, *Perceptions of corruption: Survey of Victoria Police employees* (December 2017) 9–10.

information is reiterated strongly at an early stage. The unauthorised access to a computer offences (the subject of Recommendation no.1 of this report) are not discussed with recruits.

[178] Recruits are reportedly instilled with the need to know culture with repeated references to different scenarios in which they need to assess whether they genuinely need to know (or share) information. However, the risks and dangers of – and how to avoid – grooming by persons seeking information are not specifically dealt with in any detail in current recruit or other training programs.

[179] There were hints of some possible cultural issues in the files audited by the Commission as part of this investigation. For instance, in one file the subject officer stated that: she could have asked another officer, on her behalf, to access information she was not entitled to; she could have looked it up in a hard copy file if she could not access the database; and that she had heard of others accessing information to which they were not entitled.

[180] This was countered by some examples of good practice and high integrity. Two examples were:

- a sergeant identified that a number of people possessed information that may have been obtained in an unauthorised manner from Tasmania Police. The sergeant then arranged for database checks to be run to see if anyone had accessed information to which they were not entitled, and
- a sergeant reported the unauthorised access to and potential misuse of information by a colleague. The sergeant's report displayed good awareness of policies and high integrity standards.

[181] Despite the 'grey areas' in terms of information access discussed earlier in this report, the officers conducting the Tasmania Police audits have reportedly not received excuses such as those discussed above from QPS officers. There has apparently been some negative feedback on the audits, including assertions that police are or will be too worried about being accused of unauthorised access to do their job properly. This is to be expected though.<sup>107</sup>

[182] The auditing officers report that people have generally been accepting of the process and willing to acknowledge when they have done the wrong thing. The audit focus has been on continuous professional development rather than punitive action, and people have apparently been responsive to that.

[183] In terms of recruitment processes, the Commission reviewed documentation and discussed the matter with an officer involved in recruitment. When hiring police officer recruits, Tasmania Police conducts extensive checks. This includes of prospective employees' social media accounts, and of disciplinary action taken in previous employment.

---

<sup>107</sup> See similar reports from Queensland and New Zealand in Kristian Silva, 'Queensland police criticised by union for charging veteran officer with computer hacking', *ABC News* (online), 18 July 2017; Ian Steward, 'Police computer violations exposed' *Stuff* (online) 7 December 2009.

#### **6.4. Conclusion**

[184] There did not appear to be any negative cultural issues or trends as far as the Commission could identify from its limited meetings with senior police and audits of police files.

[185] Education and training also appeared to be sufficient. Certainly recruitment processes appear to be – as one would expect given the job requirements – robust and fit for purpose.

[186] One area in which Tasmania Police could improve would be by educating employees more about grooming by persons seeking information.

## 7. Investigating and penalising abuse of information

---

[187] The way in which information abuse is investigated and penalised is reflective of whether the organisation is viewing the conduct with the required level of seriousness.

[188] There are several aspects to investigating and penalising abuse of information. For the purposes of this report, we have divided these into:

- investigating allegations – this is about whether the process used to deal with alleged information abuse is adequate
- disciplinary process outcomes – this is about whether allegations are substantiated when appropriate, and whether disciplinary actions taken are adequate, and
- pursuing prosecutions – this is about whether prosecutions are pursued when appropriate.

### 7.1. Good practice

#### **Investigating allegations**

##### *Education and awareness*

[189] When investigating allegations of information abuse, the investigator should ask the respondent about their training in, and understanding of, policies and procedures. If someone is not aware of or doesn't understand policies and procedures, it can be a mitigating factor in regard to whether misconduct has occurred.

[190] Information gained from asking these questions should also be used by the organisation to improve training, policies and procedures, and awareness raising strategies.

##### *Scope of the investigation*

[191] A checklist to safeguard against abuse of power offences for police services was released by the England and Wales police complaints oversight body in 2012.<sup>108</sup> It recommended that complaints of inappropriate sexual conduct should trigger an immediate trawling of the officer's computer use, timekeeping, and patterns of overall behaviour (as opposed to simple reactive work around the isolated incident).

##### *Removing and restricting access rights*

[192] As noted above, organisations should proactively consider suspending access to information for employees that have been accused of information abuse. A failure to

---

<sup>108</sup> Independent Police Complaints Commission, *The abuse of police powers to perpetrate sexual violence* (September 2012) 13.

do so can indicate that the organisation fails ‘to appreciate the seriousness of such behaviour’.<sup>109</sup>

[193] The Queensland CCC recommends that where it is not possible to restrict access, the ‘circumstances should be documented in the decision-making process to enhance transparency and support the decision’.<sup>110</sup>

### **Disciplinary process outcomes**

[194] Misuse of information is generally of more concern than unauthorised access to information. Where confidential information is shared, for example, ‘the employee has no way of controlling or knowing what happens with such information’.<sup>111</sup>

[195] Nonetheless, unauthorised access in and of itself can be a serious breach of privacy, is more common than misuse of information, and can lead to other forms of misconduct. There should also be ramifications where an employee has facilitated or ignored information abuse by a colleague.<sup>112</sup>

[196] Specifically in relation to predatory behaviour – which often, if not always, involves abuse of information – it has been noted that a

*[f]ailure to identify misconduct and enforce accountability for even seemingly minor indiscretions may not only empower the officer, but may also encourage those who have knowledge of, or were witness to, the behavior to commit similar or more serious offenses. Tolerance at any level will invite more of the same conduct.*<sup>113</sup>

[197] The Queensland CCC has stated that, in the public interest, it expects public sector organisations to:

- provide clear direction on access to and use of information
- ensure that these standards are consistently upheld, and
- show ‘zero tolerance’ for behaviour that does not meet the standard.<sup>114</sup>

[198] In 2005, the then Office of Police Integrity recommended that the Victoria Police commissioner advise employees that

---

<sup>109</sup> Crime and Corruption Commission Queensland, *Confidential information: Unauthorised access, disclosure and the risks of corruption in the Queensland public sector* (May 2016) 5.

<sup>110</sup> Crime and Corruption Commission Queensland, *Confidential information: Unauthorised access, disclosure and the risks of corruption in the Queensland public sector* (May 2016) 5.

<sup>111</sup> Office of Police Integrity Victoria, *Sensitive and confidential information in a police environment: Discussion paper no.2* (June 2010) 13.

<sup>112</sup> Ombudsman New South Wales, *Operation Prospect: Volume 6 Chapters 20-22 Access to and disclosure of confidential records* (December 2016) 809.

<sup>113</sup> International Association of Chiefs of Police, *Addressing Sexual Offenses and Misconduct by Law Enforcement: Executive Guide* (June 2011) 5.

<sup>114</sup> Crime and Corruption Commission Queensland, *Confidential information: Unauthorised access, disclosure and the risks of corruption in the Queensland public sector* (May 2016) 6.

*as a general policy, unauthorised access and use of information extracted from [police computer] systems will, if proven (in the absence of exceptional and extraordinary mitigation), result in dismissal'.<sup>115</sup>*

[199] This kind of zero tolerance approach appears to have been pursued by Queensland and Western Australia police for a number of years (the case of *Inglis v Pinch*<sup>116</sup> being a good example). Anecdotal reports, including advice from Tasmania Police Professional Standards Commander, indicate that WAPOL is now moving away from that approach.

[200] In any case, the outcomes of substantiated allegations should reflect the organisation's standards and policies.<sup>117</sup> Organisations should not accept implausible or inadequate excuses from employees about why they accessed information. Some of these excuses have already been discussed in this report. They include:

- a failure to provide an adequate RFA followed by an assertion that the employee cannot remember why they accessed the information
- that the employee leaves their computer logged in and someone else could have run the searches
- that it would be professionally embarrassing to be consorting with 'criminals' and so checks had to be made
- in regard to a second access, that information gained in the first access had been forgotten,<sup>118</sup> and
- that the passing on of information to a known criminal was a mere error of judgement arising out of misguided loyalty or friendship.<sup>119</sup>

### **Pursuing prosecutions**

[201] As discussed above, prosecuting unauthorised access to or misuse of information is not always in the public interest. Prosecutions are expensive, and in certain cases may not be worthwhile given the gravity of the behaviour. Evidentiary thresholds are also higher in prosecutions than in disciplinary processes.

---

<sup>115</sup> Office of Police Integrity Victoria, *Investigation into Victoria Police's Management of the Law Enforcement Assistance Program (LEAP)* (March 2005) 20–21 (Recommendation 5).

<sup>116</sup> *Inglis v Pinch* [2016] WASC 30.

<sup>117</sup> Crime and Corruption Commission Queensland, *Confidential information: Unauthorised access, disclosure and the risks of corruption in the Queensland public sector* (May 2016) 5.

<sup>118</sup> In an Australian Federal Police case, the officer said that he made the unauthorised checks because he had 'previously suffered professional embarrassment when acquaintances were the subject of criminal investigation' and that, in regard to a second access, information gained in the first access had been forgotten. The Judge stated that these excuses 'invite disbelief'. *Clancy v O'Hearn* [2011] ACTSC 117, [14]–[15], [20]–[21] (Gray J).

<sup>119</sup> In *DPP v Marks*, the Judge said that it was 'fanciful to suppose that the respondent could have believed that the provision of criminal intelligence to a known drug dealer was a "relatively innocent transfer of information" to someone to whom he felt bound by ties of friendship and loyalty. It follows that I am unable to accept that the respondent's crime should be sloughed off as a mere error of judgment, falling short of moral turpitude. In my judgment it was a serious offence.' *DPP v Marks* [2005] VSCA 277, [33] (Nettle JA).

- [202] In Victoria, the Office of Public Prosecutions has reportedly told the police service ‘on a number of occasions ... that a conviction was either unlikely or that it was equally viable to use the discipline system to deal with the matters’.<sup>120</sup>
- [203] In the case of *State of Tasmania v Johnston*, the Judge said that ‘over the years the legislature has evidenced an intent to remove, rather than broaden, the exposure of police to public prosecution in respect of disciplinary breaches’.<sup>121</sup>
- [204] However, since that case there appears to have been a marked increase in the use of the offence of misconduct in public office in other Australian jurisdictions. In 2017, the West Australian CCC was chastised for not dealing with an investigation into the unauthorised disclosure of information as criminal from the outset.<sup>122</sup>
- [205] Given community expectations and case law from other jurisdictions discussed earlier in this report, it certainly appears that prosecutions should at least be considered for public sector employees that abuse information.

## 7.2. Tasmania Police

- [206] The Commission has previously raised concerns about Tasmania Police’s handling of alleged information abuse by its officers.<sup>123</sup> In a number of complaints audited in the last few years, the Commission considered that the actions taken were too lenient, that prosecution should have been considered when it was not, or that Tasmania Police had accepted seemingly implausible excuses from its officers.
- [207] For instance, in 2014 the Commission reported on a case in which an officer had used a police database to obtain an address for a child who had been in an altercation with the officer’s child. The officer subsequently attended that child’s house on duty and in uniform, in a marked police vehicle; the officer was found to have breached the Code of Conduct, but no sanctions were imposed.<sup>124</sup>
- [208] As part of this investigation, the Commission audited 28 files supplied by Tasmania Police that contained allegations of information abuse.
- [209] This included eight ‘information only’ reports that had not been categorised as a complaint by Tasmania Police, nine Class 1 (less serious) complaints, and eleven Class 2 (more serious) complaints. Some of these matters had not been finalised at the time of the Commission’s audit.
- [210] Due to the nature of this investigation – including the limited number of files audited – the Commission’s focus was on making qualitative, not quantitative, findings.
- [211] Particular concerns the Commission had about the files were discussed at a meeting with Professional Standards in January 2018. Tasmania Police was able to resolve a

<sup>120</sup> Office of Police Integrity Victoria, *Investigation into Victoria Police’s Management of the Law Enforcement Assistance Program (LEAP)* (March 2005) 23.

<sup>121</sup> *State of Tasmania v Johnston* [2009] TASSC 60, [75] (Evans J).

<sup>122</sup> Parliamentary Inspector of the Corruption and Crime Commission of Western Australia, *Misconduct: Unauthorised disclosure of confidential information* (30 November 2017).

<sup>123</sup> For example, see Integrity Commission, *An audit of Tasmania Police complaints finalised in 2015*, Report No. 1 (2016) 8–9; Integrity Commission, *An audit of Tasmania Police complaints finalised in 2014*, Report No. 2 (2015) 57–61.

<sup>124</sup> Integrity Commission, *An audit of Tasmania Police complaints finalised in 2013*, Report No. 2 (2014) 31.

number of the Commission's concerns at that meeting. More detail on specific aspects of the handling of information abuse allegations by Tasmania Police is given below.

[212] As already discussed, the Commission did not undertake a broader survey of police or have direct access police complaint records. Both of these strategies may have provided a better understanding of how this issue is managed.

### **Investigating allegations**

#### *Education and awareness*

[213] It seems to be a relatively standard practice for Tasmania Police to ask officers interviewed as part of a misconduct investigation about their awareness and understanding of relevant policies and procedures.

#### *Scope of the investigation*

[214] In most of the audited files, the scope of the investigation and the checks run were appropriate to the circumstances.

[215] However, the categorisation of matters as 'information only' was, in most cases, curious. These matters included complaints from members of the public and police officers. The classification of a matter as an 'information only' report means that it is not included in Tasmania Police complaint statistics, and not audited by the Commission as part of its full audit process. The Commission understands that under its new complaint management system, Tasmania Police is aiming to reduce the number of matters classified as 'information only'.

#### *Removing and restricting access rights*

[216] The Commission has already suggested in this report that Tasmania Police should more proactively consider restricting information access rights for employees under investigation. In addition to the file discussed earlier, we also thought that the organisation should have considered restricting the access rights of a second officer subject to a different complaint. This was Officer Y; further details about this file are discussed below in the section about pursuing prosecutions.

[217] Officer Y did not have their access to information restricted. This was despite:

- database checks seemingly verifying allegations of extensive unauthorised access to information
- Officer Y having ongoing personal legal issues that would have made it tempting for them to misuse police databases, and
- that the complaint investigation was delayed for eight months and that Officer Y would have had means and opportunity to access the police databases extensively to assist them in their personal legal issues over that time.

[218] The flipside of this is that without being able to access Tasmania Police databases, Officer Y probably would have had to be stood down or suspended on pay for the duration of the investigation. This also would not have been a satisfactory scenario. The Commission acknowledges that there are no easy solutions in these situations.



## Disciplinary process outcomes

### *Substantiating allegations*

- [219] In some files, the Commission disagreed with Tasmania Police findings on misconduct allegations.
- [220] One example was in an 'information only' file. In that file, the officer had run searches on the owner of a venue the officer frequented. The officer ran the checks because they had heard that the owner was linked to criminal behaviour. The officer did not want to continue frequenting the venue if the owner did have criminal connections.
- [221] Although this was essentially a sustained allegation of unauthorised access, Tasmania Police found the officer's action reasonable and did not classify the file as a complaint. It was also noted that Tasmania Police did not ask the officer what actions they took when their searches verified the rumors they had heard.
- [222] In another file, three officers were found to have accessed information to which they were not entitled. However, the organisation decided not to make sustained findings for various mitigating reasons. The main mitigating reason was that the accesses occurred before 1 March 2017. This was the date that a reminder was sent out to all police about their information access obligations as part of the *Access to information awareness plan* discussed above.
- [223] Although efforts to reinforce and clarify the rules have certainly escalated over the last year or two, officers were not operating in a vacuum prior to this. One example of this is the 2005 commissioner's notice discussed earlier in this report. Another is a 2010 Police Association newsletter that stated that,
- any inappropriate disclosure by a police officer regarding confidential information or even gaining unauthorised access to confidential information is inevitably regarded as a serious breach of the Code of Conduct which may well result in significant disciplinary action regardless of the motive of the police officer involved.*<sup>125</sup>
- [224] Given this, as well as their training and other control measures (e.g. warnings that are given on database access), these three officers should have been aware of their responsibilities before 1 March 2017. In this situation, a 'not sustained' finding for two of the officers may have been borderline justifiable, but the 'exonerated' finding against the third officer was not. 'Not sustained' means that there was insufficient evidence to prove or disprove allegation; 'exonerated' means that the incident occurred but that the officer acted lawfully and properly.
- [225] A third file about which the Commission had concerns involved a male police sergeant. This file is discussed below. In addition to the 14 unauthorised accesses listed below, the male officer was found to have performed searches on ten police women in one day.
- [226] The officer explained that the searches were performed for a specific work-related purpose. Tasmania Police accepted that, while not good practice, the officer had acted

---

<sup>125</sup> Graham Wood, 'Legally speaking: police use of confidential information: issues and obligations' [December 2010] *Association News: The Official Journal of the Police Association of Tasmania* 14, 15.

in accordance with current practice at that time. Changes were made to business processes so that it would not happen again, but the officer's actions were found to be reasonable in the circumstances.

[227] However, what was not explained was why all the searches were of police women. The Commission considered it implausible that, given only a third of police are female, every single apparently random search undertaken by this officer would have been of a woman.

#### *Action taken in relation to substantiated allegations*

[228] The Commission thought that, in one file, the action taken in relation to a sustained allegation against one officer was too lenient. The matter involved two female constables and one male sergeant. The findings were that:

- one female constable accessed information related to herself unlawfully on two occasions – she received one sustained misconduct finding and verbal guidance (verbal guidance is not a sanction)
- one female constable accessed information unlawfully on six occasions – she received one sustained misconduct finding and a counselling (a counselling is the lowest form of sanction possible under the *PS Act*), and
- one male sergeant accessed information unlawfully on 14 occasions over a number of years – he received one sustained misconduct finding and a counselling.

[229] The male officer should have received a more serious sanction than a counselling. This is because of his higher rank, the extended nature of his conduct and the greater number of unlawful accesses. The action also seems unbalanced in comparison to the action taken in relation to the other two officers' misconduct.

#### **Pursuing prosecutions**

[230] As noted previously, prosecution options appear to be more limited in Tasmania than in other Australian jurisdictions. The Professional Standards Commander also told us that, in contrast to the zero tolerance approach taken in Queensland and Western Australia, Tasmania Police has a general preference for pursuing these kinds of allegations through disciplinary avenues, however that officers could lose their position (and be subject to other sanctions) through the disciplinary process, and that in any case where there is a need to consider if an officer should be charged, such matters are referred to the DPP for consideration and advice.

[231] None of the police officers in the file subject to audit by the Commission were prosecuted, although some of the matters could have been handled as potential offences. This option was generally considered by Tasmania Police – sometimes in consultation with the Director of Public Prosecutions – and a decision was made to pursue the matter through disciplinary avenues only. In most cases this decision was appropriate.

[232] There was, however, one matter in particular that the Commission thought Tasmania Police should have referred to the Director of Public Prosecutions for consideration.

This was the file concerning Officer Y, which has been mentioned above in regard to restricting access to information during an investigation.

- [233] Audits of police systems showed that Officer Y had, over many years, accessed information to which they were not entitled. The information accessed related both to Officer Y and to Officer Y's acquaintances. Subsequent interviews with Officer Y and a witness indicated that the extent of the unauthorised access to, and misuse of, information was even greater than initially suspected.
- [234] The decision was made to not deal with this file as a criminal matter because there was no criminal purpose in the unauthorised access to and misuse of information by Officer Y. That is, Officer Y was not accessing the information on behalf of, or sharing it with, criminals.
- [235] Given the breadth and extent of information abuse by Officer Y, the Commission is of the opinion that this should have been handled as a potentially criminal matter. This appears to be a classic case of considering 'police crime as a result of bad practise, lack of resources or mismanagement, rather than acts of criminals'.<sup>126</sup>
- [236] Having a criminal purpose in the information abuse would certainly have been an aggravating factor. But this does not mean that the conduct was not in and of itself potentially criminal in nature.
- [237] The Commission also noted that the leaking of information by a disgruntled employee (discussed above) may have been prosecuted, had it occurred in another jurisdiction.<sup>127</sup> The Professional Standards Commander acknowledged that prosecution options in cases such as this are limited in Tasmania, probably to official secrets in the Criminal Code, and possibly perverting the course of justice.
- [238] The Commander noted that in some instances, there were additional considerations, such as community expectations around whistle-blowers, and the messages an organisation might wish to send about 'speaking out'; however that ultimately it was always a decision for the DPP.
- [239] The Commission acknowledges these complexities. Nonetheless, it considers that an employee secretly stealing information and leaking it to certain unauthorised persons is different to a whistle-blower making a disclosure to an appropriate organisation.

### 7.3. Conclusion

- [240] The Commission found that a number of audited files were particularly well handled by Tasmania Police.

---

<sup>126</sup> Petter Gottschalk and Siri Stedje, 'Crime and motive as predictors of jail sentence for police misconduct' (2010) 38 *International Journal of Law, Crime and Justice* 49, 49, 50.

<sup>127</sup> For examples of, and discussions about, police allegedly leaking information to the media, see *R v Martin* [2017] SADC 73, especially paragraphs [23]–[26] (Tilmouth J); Rebecca Opie, 'Media leaks detective Peter Martin found not guilty of seven corruption charges', *ABC News* (online), 23 October 2017; Rebecca Opie, 'Prosecutors drop remaining corruption charges against SA detective accused of media leaks', *ABC News* (online), 24 November 2017; Petter Gottschalk, 'Crime-based survey instrument for police integrity measurement' (2010) 33(1) *Policing: An International Journal of Police Strategies & Management* 52, 56; *R v Chapman* [2015] QB 833; Laura Tidey, 'Rogers v Television New Zealand Ltd: Police and the Release of Information to the Media' (2009) 40 *Victoria University of Wellington Law Review* 507; Office of Police Integrity Victoria, *Sensitive and confidential information in a police environment: Discussion paper no.2* (June 2010), especially at 14.

- [241] Where the Commission had concerns, these were mainly around the substantiation of allegations. Especially in light of the strategies implemented as part of its *Access to information awareness plan*, in future Tasmania Police should more stringently enforce policies and standards.
- [242] In regard to prosecutions, the difference in approach in comparison to other jurisdictions may be substantially attributable to the differences in legislation discussed earlier in this report. Whether this is a situation that needs to be remedied is a decision for the Parliament of Tasmania.
- [243] Nonetheless, Tasmanian public sector organisations need to understand that unauthorised access and misuse of information is serious in and of itself. The employee does not need to be accessing the information on behalf of criminal organisations for the conduct to be viewed as extremely serious and potentially criminal.

## 8. Concluding remarks

---

[244] Technological advances have led to an increase in the amount of personal and sensitive information held by public sector organisations. While this has increased efficiency, it has also led to the creation of a high misconduct risk area.

[245] While focusing on Tasmania Police, it is intended that this report will result in broader learnings applicable across the public sector. Organisations should view their information holdings as significant assets worthy of high levels of protection, and vulnerable to abuse. Public sector employees are the custodians of that information – not the owners – and they have no right to use the information for their own personal purposes, regardless of the motivation.

[246] It is essential that organisations recognise the risks and take steps to protect the information they hold. This includes by:

- establishing simple and clear policies and procedures
- having adequate information security measures in place
- cultivating good organisational culture and awareness around information management responsibilities, and
- enforcing policies and procedures.

[247] Given the breadth and sensitivity of information they hold, police services must meet these requirements in order to maintain credibility and public trust.

[248] The Commission has found that, overall, Tasmania Police has adequate policies, procedures and information security measures in place. Especially with the recently implemented audit program, it appears to be cultivating good organisational culture and awareness around information management responsibilities.

[249] In future Tasmania Police should more strictly enforce policies and procedures when officers are found to have done the wrong thing. Police need to understand the importance of maintaining high standards in regard to information access and use.

[250] In regard to prosecutions, it does appear that Tasmania Police – and Tasmania more generally – has a different approach to other Australian jurisdictions. It is a question for the Parliament of Tasmania as to whether it should be easier to prosecute public sector employees for serious information abuse in this state.

## Appendix A – References

---

- 'Corrupt AFP officer Benjamin Hampton jailed for 11 months', *Australian Associated Press* (online) 22 November 2017
- 'Disgraced cop escapes jail over computer hack', *Australian Associated Press* (online), 18 November 2009
- 'Former police officer avoids jail over computer offence', *ABC News* (online), 18 November 2009
- 'Queensland ex-cop Peter Betts fined \$8k, spared jail after sharing confidential information', *ABC News* (online), 14 March 2016
- 'Sex was cop's motive in accessing information, court told', *Australian Associated Press* (online), 17 November 2009
- Arnold, Bruce, 'Case note: Clancy v O'Hearn' [September 2011] *Privacy Law Bulletin* 38
- Australian Commission for Law Enforcement Integrity, *ACLEI Top 5 Corruption Prevention Myths* (Undated) <[www.aclei.gov.au/corruption-prevention/corruption-prevention-myths](http://www.aclei.gov.au/corruption-prevention/corruption-prevention-myths)>
- Australian Commission for Law Enforcement Integrity, *Identifying corruption risk* (Undated) Corruption Prevention Toolkit <[www.aclei.gov.au/corruption-prevention/corruption-prevention-toolkit/identifying-corruption-risk](http://www.aclei.gov.au/corruption-prevention/corruption-prevention-toolkit/identifying-corruption-risk)>
- Australian Commission for Law Enforcement Integrity, *Internal corruption controls used by law enforcement agencies* (Undated) <[www.aclei.gov.au/integrity-framework-checklist-law-enforcement-agencies](http://www.aclei.gov.au/integrity-framework-checklist-law-enforcement-agencies)>
- Australian Commission for Law Enforcement Integrity, *Investigation Report: An investigation into the conduct of an Australian Federal Police appointee in relation to unauthorised disclosure of information and the giving of testimonials (Report 03/2012)* (17 October 2012)
- Australian Commission for Law Enforcement Integrity, *Investigation Report: Operation Galaxy — A joint investigation into the conduct of an Australian Crime Commission ICT staff member (Report 01/2016)* (15 January 2016)
- Australian Commission for Law Enforcement Integrity, *Investigation Report: Operation Marlowe—A joint investigation into the conduct of an Australian Federal Police Protective Service Officer concerning information security (Report 01/2017)* (5 May 2017)
- Australian Commission for Law Enforcement Integrity, *Summary of report 03/2016* (2016)
- Australian Commission for Law Enforcement Integrity, *Summary of report 03/2013* (2013)
- Australian Commission for Law Enforcement Integrity, *Summary of Report 01/2012* (2012)
- Australian Federal Police, 'Adjudication of a Category 3 Conduct Issue (73487; 8022; 2015/1963)' (September 2016) *AFP RTI information release - 18-2017 - Request for documents in relation to the misuse of PROMIS or RAPID systems by ACT Policing members (FOI - CRM 2017/460)* <[www.afp.gov.au/about-us/information-publication-scheme/routinely-requested-information-and-disclosure-log](http://www.afp.gov.au/about-us/information-publication-scheme/routinely-requested-information-and-disclosure-log)>
- Australian Federal Police, *AFP National Guideline on information management* (Undated) <[www.afp.gov.au/about-us/information-publication-scheme](http://www.afp.gov.au/about-us/information-publication-scheme)>

Australian Federal Police, *AFP National Guideline on the security of information systems* (Undated) <[www.afp.gov.au/about-us/information-publication-scheme](http://www.afp.gov.au/about-us/information-publication-scheme)>

Australian Federal Police, *AFP National Guideline on the security of ICT system access* (Undated) <[www.afp.gov.au/about-us/information-publication-scheme](http://www.afp.gov.au/about-us/information-publication-scheme)>

Australian Institute of Criminology, 'Hacking offences' (2005) 05 *High Tech Crime Brief*

Australian Public Service Commission, *Section 4: Managing information* (17 February 2016)  
APS Values and Code of Conduct <[www.apsc.gov.au/publications-and-media/current-publications/values-and-conduct/managing-information](http://www.apsc.gov.au/publications-and-media/current-publications/values-and-conduct/managing-information)>

Australian Securities & Investments Commission, *Consultation Paper 128: Handling confidential information* (December 2009)

College of Policing, *Information management* (23 October 2013) Authorised Professional Practice <[www.app.college.police.uk/app-content/information-management/](http://www.app.college.police.uk/app-content/information-management/)>

Commonwealth Director of Public Prosecutions, 'Federal police officer gaoled for corruption' (Media Release, 22 November 2017)

Commonwealth Director of Public Prosecutions, *Practice Group Instruction Number 2: Computer Browsing offences under the Criminal Code* (3 September 2014)  
<[www.cdpp.gov.au/crimes-we-prosecute/general-prosecutions](http://www.cdpp.gov.au/crimes-we-prosecute/general-prosecutions)>

Commonwealth Director of Public Prosecutions, *Prosecution Policy of the Commonwealth: Guidelines for the Making of Decisions in the Prosecution Process* (Undated)  
<[www.cdpp.gov.au/prosecution-process/prosecution-policy](http://www.cdpp.gov.au/prosecution-process/prosecution-policy)>

Corruption and Crime Commission Western Australia, *The CCC relies on good people doing the right thing – Stacey* (5 December 2017) News Archive 2017  
<[www.ccc.wa.gov.au/news/445](http://www.ccc.wa.gov.au/news/445)>

Cox, William, *Report of the Independent Reviewer* (May 2016) Independent Review of the Integrity Commission Act 2009

Crime and Corruption Commission Queensland, 'CCC serves Brisbane policeman with a notice to appear in court for misusing database - 13 June' (Media Release, 13 June 2017)

Crime and Corruption Commission Queensland, 'CCC urges Queensland public servants to adhere to privacy rules - 17 May 2017' (Media Release, 17 May 2017)

Crime and Corruption Commission Queensland, 'Central region police officer charged with criminal offences - 15 November 2016' (Media Release, 15 November 2016)

Crime and Corruption Commission Queensland, 'Former Brisbane police officer to appear in court for misusing confidential information - 28 June' (Media Release, 28 June 2017)

Crime and Corruption Commission Queensland, 'Police officer charged for unauthorised access and disclosure of confidential information - 22 June 2016' (Media Release, 22 June 2016)

Crime and Corruption Commission Queensland, *Confidential information: Unauthorised access, disclosure and the risks of corruption in the Queensland public sector* (May 2016)

Crime and Corruption Commission Queensland, *Corruption Prevention Advisory: Information security and handling* (September 2016)

Crime and Corruption Commission Queensland, *Corruption Prevention Advisory: Management of public records – Advice for all employees of a public authority* (July 2017)

Crime and Corruption Commission Queensland, *Corruption Prevention Advisory: Use of official resources* (July 2017)

Crime and Corruption Commission Queensland, *How to respond to a confidential information incident in your agency: A six-step guide for managers and supervisors* (November 2016)

Crime and Misconduct Commission Queensland, *Monitoring police ethics: a 2013 survey of Queensland recruits and First Year Constables* (October 2013) Research and Issues Paper Number 13

Criminal Justice Commission Queensland, *Protecting Confidential Information: A Report on the Improper Access to, and Release of, Confidential Information from the Police Computer Systems by Members of the Queensland Police Service* (November 2000)

Davids, Cindy and Marilyn McMahon, 'Police Misconduct as a Breach of Public Trust: The Offence of Misconduct in Public Office' (2014) 19(1) *Deakin Law Review* 89

Department of Police, Fire and Emergency Management (Tasmanian Government), *2017-2020 Future Focus* (Undated) <[www.police.tas.gov.au/historical-corporate-documents/future-focus-2017-2020/](http://www.police.tas.gov.au/historical-corporate-documents/future-focus-2017-2020/)>

Easton, Stephen 'Privacy lessons for public service apps: two good examples and one failure', *The Mandarin* (online) 1 September 2017

Gottschalk, Petter and Siri Stedje, 'Crime and motive as predictors of jail sentence for police misconduct' (2010) 38 *International Journal of Law, Crime and Justice* 49

Gottschalk, Petter, 'Crime-based survey instrument for police integrity measurement' (2010) 33(1) *Policing: An International Journal of Police Strategies & Management* 52

Gottschalk, Petter, 'Management challenges in law enforcement: the case of police misconduct and crime' (2011) 53(3) *International Journal of Law and Management* 169

Gottschalk, Petter, 'Policing police crime: the case of criminals in the Norwegian police' (2009) 11(4) *International Journal of Police Science and Management* 429

Independent Broad-based Anti-Corruption Commission, *Perceptions of corruption: Survey of Victoria Police employees* (December 2017)

Independent Broad-based Anti-Corruption Commission, *Predatory behaviour by Victoria Police officers against vulnerable persons: Intelligence report 2* (December 2015)

Independent Commission Against Corruption New South Wales, *Confidential information* (Undated) Preventing Corruption <[www.icac.nsw.gov.au/preventing-corruption/known-your-risks/confidential-information/4913](http://www.icac.nsw.gov.au/preventing-corruption/known-your-risks/confidential-information/4913)>

Independent Commission Against Corruption New South Wales, *IT systems* (Undated) Preventing Corruption <[www.icac.nsw.gov.au/preventing-corruption/known-your-risks/it-systems/4911](http://www.icac.nsw.gov.au/preventing-corruption/known-your-risks/it-systems/4911)>

Independent Commission Against Corruption New South Wales, *Tip sheet for employees: Use and misuse of public sector resources* (February 2008)



Independent Police Complaints Commission, *The abuse of police powers to perpetrate sexual violence* (September 2012)

Integrity Commission, *An audit of Tasmania Police complaints finalised in 2013*, Report No. 2 (2014)

Integrity Commission, *An audit of Tasmania Police complaints finalised in 2014*, Report No. 2 (2015)

Integrity Commission, *An audit of Tasmania Police complaints finalised in 2015*, Report No. 1 (2016)

Integrity Commission, *Prosecuting serious misconduct in Tasmania: The missing link – Interjurisdictional review of the offence of 'misconduct in public office* (October 2014)

Integrity Commission, Submission to Independent Review, *Integrity Commission Act Review*, March 2016, <[www.integrity.tas.gov.au/reports\\_and\\_publications/reviews](http://www.integrity.tas.gov.au/reports_and_publications/reviews)>

Integrity Commission, *Submission to the Three Year Review* (2013), volume 1 <[www.integrity.tas.gov.au/reports\\_and\\_publications/reviews](http://www.integrity.tas.gov.au/reports_and_publications/reviews)>

International Association of Chiefs of Police, *Addressing Sexual Offenses and Misconduct by Law Enforcement: Executive Guide* (June 2011)

International Association of Chiefs of Police, *IACP Technology Policy Framework* (January 2014)

Kidd, Jessica, 'Former AFP officer Ben Hampton jailed for selling secret information', *ABC News* (online) 23 November 2017

Kohlbacher, Sonia, 'Fmr Qld cop to face court for misconduct', *Australian Associated Press* (online) 28 June 2017

LexisNexis, Criminal Law WA (at 16 April 2018)

Liedtka, Jeanne M, 'Value Congruence: The Interplay of Individual and Organizational Value Systems' (1989) 8(10) *Journal of Business Ethics* 805

Mills, Tammy, 'We are deeply sorry': Victoria Police apologises for what happened to Michael Maynes', *The Age* (online) 17 January 2018

New South Wales Police Force, *Privacy Management Plan* (2013) <[www.police.nsw.gov.au/about\\_us/policies\\_procedures\\_and\\_legislation](http://www.police.nsw.gov.au/about_us/policies_procedures_and_legislation)>

New Zealand Police, *Our Code* (2015) <[www.police.govt.nz/about-us/publication/new-zealand-police-code-conduct](http://www.police.govt.nz/about-us/publication/new-zealand-police-code-conduct)>

Noone, Richard 'Scorned woman uses cop database to harass lover', *The Daily Telegraph* (online), 21 December 2016

Oakes, Dan, 'Former VicRoads worker illegally supplied information from agency's database', *ABC News* (online), 5 March 2018

Oakes, Dan, 'VicRoads worker charged by anti-corruption commission over alleged data breaches', *ABC Radio Australia* (online), 19 January 2018

Office of Police Integrity Victoria, *Assessing unauthorised and inappropriate emails: Guidelines for assessors* (July 2010)

Office of Police Integrity Victoria, *Assessing unauthorised and inappropriate emails: A tool for determining risk* (July 2010)

Office of Police Integrity Victoria, *Information Security and the Victoria Police State Surveillance Unit* (February 2010)

Office of Police Integrity Victoria, *Investigation into Victoria Police's Management of the Law Enforcement Assistance Program (LEAP)* (March 2005)

Office of Police Integrity Victoria, *Report on the Leak of a Sensitive Victoria Police Information Report* (February 2005)

Office of Police Integrity Victoria, *Sensitive and confidential information in a police environment: Discussion paper no.2* (June 2010)

Office of the Australian Information Commissioner, *Guide to information security* (April 2013)

Ombudsman New South Wales, *Operation Prospect: Volume 6 Chapters 20-22 Access to and disclosure of confidential records* (December 2016)

Ombudsman New South Wales, *Sector Agencies Fact Sheet 19: Security of information* (March 2012)

Ombudsman Victoria, *Whistleblowers Protection Act 2001 Investigation into the disclosure of information by a councillor of the City of Casey* (March 2010)

Opie, Rebecca, 'Media leaks detective Peter Martin found not guilty of seven corruption charges', *ABC News* (online), 23 October 2017

Opie, Rebecca, 'Prosecutors drop remaining corruption charges against SA detective accused of media leaks', *ABC News* (online), 24 November 2017

Parliamentary Inspector of the Corruption and Crime Commission of Western Australia, *Misconduct: Unauthorised disclosure of confidential information* (30 November 2017)

People, Julie, 'Research and Issues Papers Number 02: Unauthorised Disclosure of Confidential Information by NSW Police Officers' (October 2008) *Police Integrity Commission New South Wales*

Petrinec, Melanie, 'Former drug squad cop Peter Betts fined for misusing police computer system', *Gold Coast Bulletin* (online), 14 March 2016

Public Sector Commission, *Public Sector Commissioner's Circular 2010-05: Computer Information and Internet Security* (16 April 2010) <[publicsector.wa.gov.au/document/public-sector-commissioners-circular-2010-05-computer-information-and-internet-security](http://publicsector.wa.gov.au/document/public-sector-commissioners-circular-2010-05-computer-information-and-internet-security)>

Queensland Police Service, *Management Support Manual* (29 March 2018) <[www.police.qld.gov.au/corporatedocs/OperationalPolicies/msm.htm](http://www.police.qld.gov.au/corporatedocs/OperationalPolicies/msm.htm)>

Rigney, Sam, 'Police officer Donna Michelle Sharpe pleads guilty to hindering an investigation and perverting the course of justice over partner's boat theft', *The Advocate* (online), 2 March 2018

Secretary of State for the Home Department/National Centre for Policing Excellence, *Code of Practice on the Management of Police Information* (July 2005) <[library.college.police.uk/docs/APPref/Management-of-Police-Information.pdf](http://library.college.police.uk/docs/APPref/Management-of-Police-Information.pdf)>

Silva, Kristian, 'Queensland police criticised by union for charging veteran officer with computer hacking', *ABC News* (online), 18 July 2017

Smith, David and Tim Lee, 'When there is a breach – Know your obligations and what steps to take' (2015) 88 *Computers & Law* 1

Steward, Ian, 'Police computer violations exposed' *Stuff* (online) 7 December 2009

Tidey, Laura, 'Rogers v Television New Zealand Ltd: Police and the Release of Information to the Media' (2009) 40 *Victoria University of Wellington Law Review* 507

Victorian Ombudsman, *Investigation into the improper release of autopsy information by a Victorian Institute of Forensic Medicine employee Whistleblowers Protection Act 2001* (May 2011)

Weber, David, 'WA prison officer fend for using Corrective Services computer to get information about inmates', *ABC News* (online), 6 August 2015

Western Australia Police, *Code of Conduct* (August 2010)

Wood, Graham, 'Legally speaking: police use of confidential information: issues and obligations' [December 2010] *Association News: The Official Journal of the Police Association of Tasmania* 14

## **Cases**

*AB & Anor, R (on the application of) v North Wales Police Area* [1998] EWCA Civ 486

*Casilli v Wehrmann* [2014] WASC 319

*Clancy v O'Hearn* [2011] ACTSC 117

*Cogan v Velkovski* [2016] WASC 158

*D'Alo v Nolan* [2006] VSC 362

*DPP v Artz* [2013] VCC 56

*DPP v Marks* [2005] VSCA 277

*DPP v Zierk* [2008] VSC 184

*Hughes v R* [2014] NSWCCA 15

*Hull v The State of Western Australia* [2005] WASCA 194

*Inglis v Pinch* [2016] WASC 30

*Jansen v Regina* [2013] NSWCCA 301

*Macdonald v Commissioner of Police* [2017] NSWIRComm 1070

*Queensland Police Service v Neuman* [2017] QMC 6

*Question of Law Reserved (No. 2 of 1996)* (1996) 67 SASR 63

*R v Austin* [2013] SASCFC 133

*R v Bunning* [2007] VSCA 205

*R v Chapman* [2015] QB 833

*R v Huy Vinh Quach* [2010] VSCA 106

*R v Martin* [2017] SADC 73

*Rhatigan v Forbes* [2009] WASC 368

*State of Tasmania v Johnston* [2009] TASSC 60

*Taylor v The State of Western Australia* [2015] WASCA 72

*The State of Western Australia v Burke* [2011] WASCA 190

Transcript of Proceedings, *State of Tasmania v Johnston* [2009] HCATrans 330 (11 December 2009)

### **Legislation**

*Australian Federal Police Act 1979* (Cth)

*Criminal Code Act 1924* (Tas)

Explanatory Memorandum, National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017 (Cth)

*Integrity Commission Act 2009* (Tas)

National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017 (Cth)

*Police Administration Act* (NT)

*Police Force Regulations 1979* (WA)

*Police Regulations 2014* (SA)

*Police Service Act 2003* (Tas)

*Police Service Administration Act 1990* (Qld)

*Victoria Police Act 2013* (Vic)

## Appendix B – Information abuse offences across Australia

Offences listed below are those that most closely characterise the heading offence. There are a number of other potentially relevant or closely related offences that are not included in this table.

	Australian Capital Territory (ACT)	Commonwealth (Cth)	Northern Territory (NT)	New South Wales (NSW)	Queensland (Qld)	South Australia (SA)	Tasmania (Tas)	Victoria (Vic)	Western Australia (WA)
<b>Misconduct in public office</b>	<i>Criminal Code 2002 (ACT)</i> s 359 – 'Abuse of public office'	<i>Criminal Code Act 1995 (Cth)</i> s 142.2 – 'Abuse of public office'	<i>Criminal Code Act 1983 (NT)</i> s 82 – 'Abuse of office'	Common law offence of misconduct in public office	<i>Criminal Code Act 1899 (Qld)</i> s 92 – 'Abuse of office'  <i>Criminal Code Act 1899 (Qld)</i> s 92A – 'Misconduct in relation to public office'	<i>Criminal Law Consolidation Act 1935 (SA)</i> s 251 – 'Abuse of public office'	Nil - <i>Criminal Code Act 1924 (Tas)</i> s 253A – 'Fraud' may apply	Common law offence of misconduct in public office	<i>Criminal Code Act Compilation Act 1913 (WA)</i> s 83 – 'Corruption'
<b>Official corruption or bribery</b>	<i>Criminal Code 2002 (ACT)</i> s 356 – 'Bribery'  <i>Criminal Code 2002 (ACT)</i> s 357 – 'Other corrupting benefits'	<i>Criminal Code Act 1995 (Cth)</i> s 141.1 – 'Bribery of a Commonwealth public official'  <i>Criminal Code Act 1995 (Cth)</i> s 142.1 – 'Corrupting benefits given to, or received by, a Commonwealth public official'	<i>Criminal Code Act 1983 (NT)</i> s 77 – 'Official corruption'	Common law offences may apply  <i>Police Act 1990 (NSW)</i> s 200 – 'Bribery or corruption' (Note that this offence is specific to police officers.)	<i>Criminal Code Act 1899 (Qld)</i> s 87 – 'Official corruption'	<i>Criminal Law Consolidation Act 1935 (SA)</i> s 249 – 'Bribery or corruption of public officers'  <i>Criminal Law Consolidation Act 1935 (SA)</i> s 252 – 'Demanding or requiring benefit on basis of public office'  <i>Criminal Law Consolidation Act 1935 (SA)</i> s 253 – 'Offences relating to	<i>Criminal Code Act 1924 (Tas)</i> s 83 – 'Corruption of public officers'	<i>Secret commission offences in Crimes Act 1958 (Vic)</i> ss 176–180  <i>Victoria Police Act 2013 (Vic)</i> s 252 – 'Bribery and corruption by police or protective services officers'  <i>Victoria Police Act 2013 (Vic)</i> s 253 – 'Bribery and corruption towards police or protective	<i>Criminal Code Act Compilation Act 1913 (WA)</i> s 82 – 'Bribery of public officer'

	Australian Capital Territory (ACT)	Commonwealth (Cth)	Northern Territory (NT)	New South Wales (NSW)	Queensland (Qld)	South Australia (SA)	Tasmania (Tas)	Victoria (Vic)	Western Australia (WA)
						appointment to public office'		services officers' (Note that the above two offences are specific to police officers.)	
<b>Computer hacking or unauthorised access to information</b>	<i>Criminal Code 2002</i> (ACT) s 420 – 'Unauthorised access to or modification of restricted data held in computer'	<i>Criminal Code Act 1995</i> (Cth) s 478.1 – 'Unauthorised access to, or modification of, restricted data'  <i>Crimes Act 1914</i> (Cth) s 308H – 'Unauthorised access to or modification of restricted data held in computer (summary offence)'	<i>Criminal Code Act 1983</i> (NT) s 222 – 'Unlawfully obtaining confidential information'  <i>Criminal Code Act 1983</i> (NT) s 276B – 'Unlawful access to data'  <i>Criminal Code Act 1983</i> (NT) s 276C – 'Unlawful modification of data'	<i>Crimes Act 1900</i> (NSW) s 308H – 'Unauthorised access to or modification of restricted data held in computer (summary offence)'	<i>Criminal Code Act 1899</i> (Qld) s 408E – 'Computer hacking and misuse'	<i>Summary Offences Act 1953</i> (SA) s 44 – 'Unlawful operation of computer system'  <i>Criminal Law Consolidation Act 1935</i> (SA) s 86G – 'Unauthorised modification of computer data'	<i>Criminal Code Act 1924</i> (Tas) s 257C – 'Damaging computer data'  <i>Criminal Code Act 1924</i> (Tas) s 257D – 'Unauthorized access to a computer'  <i>Criminal Code Act 1924</i> (Tas) s 257E – 'Insertion of false information as data'  <i>Police Offences Act 1935</i> (Tas) s 43C – 'Unauthorized access to a computer'	<i>Crimes Act 1958</i> (Vic) s 247G – 'Unauthorised access to or modification of restricted data'	<i>Criminal Code Act Compilation 1913</i> (WA) s 440A – 'Unlawful use of computer'
<b>Disclosure of official secrets</b>	<i>Crimes Act 1900</i> (ACT) s 153 – 'Disclosure of information by territory officer'	<i>Crimes Act 1914</i> (Cth) s 70 – 'Disclosure of information by Commonwealth officers' (Note that a bill is currently before the Parliament)	<i>Criminal Code Act 1983</i> (NT) s 76 – 'Disclosure of official secrets'	Common law offences may apply	<i>Criminal Code Act 1899</i> (Qld) s 85 – 'Disclosure of official secrets'	Common law offences may apply	<i>Criminal Code Act 1924</i> (Tas) s 110 – 'Disclosure of official secrets'	Common law offences may apply	<i>Criminal Code Act Compilation 1913</i> (WA) s 81 – 'Disclosing official secrets'

	Australian Capital Territory (ACT)	Commonwealth (Cth)	Northern Territory (NT)	New South Wales (NSW)	Queensland (Qld)	South Australia (SA)	Tasmania (Tas)	Victoria (Vic)	Western Australia (WA)
		<i>which would see this section replaced – see National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017.)</i>							
<b>Information abuse offences created under police service legislation</b>	See Cth.	<i>Australian Federal Police Act 1979 (Cth) s 60A – ‘Secrecy’</i>	<i>Police Administration Act (NT) s 155 – ‘Communication of information’</i>	<i>Police Regulation 2008 (NSW) reg 75 – ‘Confidential information’</i>	<i>Police Service Administration Act 1990 (Qld) s 10.1 – ‘Improper disclosure of information’</i>	<i>Police Regulations 2014 (SA) reg 93 – ‘Offence for former employees in the department to use or disclose information’</i>	Nil	<i>Victoria Police Act 2013 (Vic) ss 225–232</i>	Nil

## **Appendix C – Submission of Tasmania Police**

---



OFFICE OF THE COMMISSIONER  
47 Liverpool Street Hobart  
[GPO Box 308]  
HOBART TAS 7001  
Phone (03) 6230 2111  
Fax (03) 6230 2117

Our Ref: A18/81702  
Your Ref:  
Enquiries:



18 May 2018

Mr R Bingham  
Chief Executive Officer  
Integrity Commission  
Level 2 - 199 Macquarie Street  
HOBART TAS 7000

Dear Mr Bingham,

#### **OWN-MOTION INVESTIGATION MM17/0098**

Thank you for the opportunity to review the draft report of the Commission's Own-Motion Investigation and to provide comment.

It is pleasing to note that the Commission found that, overall, Tasmania Police policies, practices and procedures governing the management of information are adequate, appropriate, and generally meet good practice standards. While Tasmania Police does not necessarily support the views of the Commission in every aspect arising from the investigation, as an organisation we are always looking for opportunities to improve our information management arrangements. To that end, we will ensure that the Commission's final report is comprehensively reviewed and any necessary changes to policy or procedures implemented.

Tasmania Police has robust information management arrangements and compliance is strictly enforced. We have invested significantly in educating and training our officers and other staff in relevant legislative and policy requirements and raising awareness of what does and what does not constitute legitimate systems access. Breaches of relevant orders, policy and procedures are viewed seriously and action, including sanctions for inappropriate and authorised access and disclosure, are implemented as required.

It is prudent that I specifically comment on one aspect contained within the Commission's report, namely the issue of direct access to the Tasmania Police complaints database. The Commission's position on that issue is well known but not supported by Tasmania Police. The reasons why direct access has not been allowed have previously been communicated to the Commission on a number of occasions and remain valid and unchanged in our view. In this case, the Commission was provided with all information it requested and there was a high level of cooperation and liaison between Commission staff and relevant members of Tasmania Police, particularly the Professional Standards Command. I am not aware of any issues associated with the Commission's access to the information it needed to conduct its

investigation, other than its preference to have direct access, but please feel free to raise any particular concerns if indeed that was the case.

The Commander, Professional Standards, has prepared a report to the Deputy Commissioner's office in which he provides more detailed comments in relation to the draft investigation report and I have arranged for a copy of that report to be emailed to Mr Michael Easton of your office for consideration in developing the final version. It is not requested that the Commander's report be published as part of the Commission's report. It is supplied solely for the purpose of assisting the Commission in its deliberations while finalising the document.

Thank you again for the opportunity to provide comments.

Yours sincerely



**S A TILYARD**  
Acting Commissioner of Police

## **Appendix D – Submission of Director of Public Prosecutions**

---



OFFICE OF THE DIRECTOR OF PUBLIC PROSECUTIONS

INQUIRIES: Daryl Coates SC  
OUR REF: 31060  
YOUR REF: MM17/0098

RECEIVED

15 MAY 2018

10 May 2018

Mr Richard Bingham  
Chief Executive Officer  
Integrity Commission  
GPO Box 822  
Hobart Tasmania 7001

Dear Mr Bingham

**OWN MOTION INVESTIGATION – TASMANIA POLICE USE OF INFORMATION**

Thank you for your letter of 9 May 2018.

I am generally content with your amendments to the report.

In respect to [71]-[73] in your attachment at p 4, my position is that a police officer or public servant only has authority to access a computer or part of a computer system pursuant to s 257D for work purposes. They have no authority to access it for a non-work purpose. Therefore, if they do it for a non-work purpose they have no lawful excuse and therefore they have committed an offence under s 257D of the *Criminal Code*. However, I do accept the Commission's view that there is uncertainty in respect to the interpretation and it would be useful to clarify that with legislation.

The case I was referring to at our meeting was *Tasmania v Tania Clarke*. Ms Clark was sentenced on 15 February 2008 by Crawford J and received six months' imprisonment wholly suspended. She pleaded guilty to two counts of disclosing official secrets. I attached a copy of the comments on passing sentence. Obviously, this case was prior to *Tasmania v Johnston* [2009] TASSC 60. Given the problems identified in the Johnston case, if this case occurred now I would probably prosecute under s 257D of the *Criminal Code*. However, it only covers the conduct of accessing the information. It does not effectively cover the conduct of disclosing it. This would highlight the need to revamp s 110 of the *Criminal Code*.

If you have any other queries, please do not hesitate to contact me.

Yours sincerely

D G Coates SC

**DIRECTOR OF PUBLIC PROSECUTIONS**

SentResult2 ▾ &lt; &lt;&lt;

**Name**

Clarke, Tania Eirene

**Sentence**

TASMANIA v TANIA EIRENE CLARKE 15 FEBRUARY 2008  
COMMENTS ON PASSING SENTENCE CRAWFORD J

There were two counts of disclosing official secrets against Tania Eirene Clarke. She has pleaded guilty to them both.

I will summarise the facts but not deal with them in too much detail because they have just been stated to the Court. She had been a police officer for only about a month when she formed a relationship with a man who had a record, although I understand unknown to her at the time. He had previously been involved in drugs in Victoria and had come to this State. She fell in love with him and in the course of her relationship with him she became suspicious about something concerning him, largely because he was having extended absences without explanation. In August 2006 she breached her duty as a police officer by entering its computer information system and obtained information concerning him. It included that he had been found by police at business premises with another person in suspicious circumstances and that he had a record in Victoria. With that information she confronted him, not for the purpose of obstructing an investigation, but in her own interests arising out of her relationship with him. He gave her an explanation for those matters which she accepted and the relationship continued.

In March 2007 she again accessed the information system in breach of her duty as a police officer. She ascertained that it was believed that he was in the business of dealing in drugs and perhaps the manufacture of them and she confronted him with that information, again not for the purpose of obstructing any ongoing investigation concerning him but because of her relationship with him and her affection for him. Once again he gave her an explanation which she foolishly accepted.

About a month or two later all was revealed. Internal investigation revealed what she had done and on being interviewed she confessed to it.

She is a person who is otherwise of good character. She had many years in the Royal Navy and she has had a good working life. There is no reason to think that these crimes were other than out of character. There is no reason to think that they would have occurred if it had not been for her love or infatuation, whatever it was, for this man, who was continually lying to her about himself and generally.

As a result of this she has lost her occupation as a police officer and she will obviously have difficulty obtaining an employment position in a public office, so she has suffered substantial punishment as a result of her conduct.

It is a relatively serious crime and if it had been committed by an active police officer with a mind to pervert justice or obstruct an ongoing investigation, actual imprisonment would be the only appropriate punishment. Because it is a serious offence a sentence of imprisonment is appropriate but it will all be suspended having regard to the unique circumstances of the case. I suppose any case like this is unique because so far as my investigations reveal, there has been no charge of this crime in the last 20 years and I can find no record of one at all.

The orders of the Court will be as follows. A conviction is recorded on both counts. The victims of crime compensation levies of \$100 are directed to be paid within one month. She is sentenced to 6 months' imprisonment but all of that is suspended upon condition that she is of good behaviour for the next three years.

The sentence is one of imprisonment to mark the Court's condemnation of actions by a police officer involving such serious breaches of her duty.

2

SentResult2 ▾ &lt; &lt;&lt;

---

Powered by DB/Text *WebPublisher*, from **INMAGIC**

## **Appendix E – Submission of Police Association of Tasmania**

---



## **POLICE ASSOCIATION OF TASMANIA**

Founded 1923

*Unity  
Equity  
Friendship*

All correspondence to  
be addressed to:

The General Secretary  
Mark Kadziolka

107 New Town Road,  
New Town,  
Tasmania 7008.

Telephone: 03 6278 1900  
Facsimile: 03 6278 1315  
Email: [pat@pat.asn.au](mailto:pat@pat.asn.au)  
Web: <http://www.pat.asn.au>  
ABN: 37 480 634 459

16 May 2018

Mr Richard Bingham  
Chief Executive Officer  
Integrity Commission  
Level 2/199 Macquarie Street  
HOBART TAS 7000

Dear Mr Bingham

### **Own-motion investigation MM17/0098**

Thank you for the opportunity to comment on the above own motion investigation regarding Tasmania Police's handling of members of the Police Service accessing information.

Firstly, information is necessary for the proper functioning of the Police Service to effectively detect and prosecute offenders and protect the community. Information relevant to policing about an individual's activity may be in the eyes of some members of the community a sacrosanct possession, but to police officers it is considered as necessary intelligence and is clearly an effective tool required to carry out their day to day duties. While public sensitivities may exist regarding the use of information, police officers balance this with use of it for the betterment of society.

While we are not advocating unrestricted access to all information, we are strongly adhering to the view that the best judge of whether information is legitimately accessed for policing purposes is the Police Service because it understands the intricacies of law enforcement. We understand the variety of opinions on this matter but are settled on the practical view that not everyone can be satisfied ultimately, and therefore we are inclined towards what is best for policing and society.

The PAT still maintains the position previously expressed to officers of the Integrity Commission (the Commission) that there are other entities far more deserving of your attention, especially when your organisation has expressed previously the need for more resources to fulfil its remit.

Tasmania Police is the most accountable organisation in Tasmania with an exemplary record of investigating and dealing with wrongdoing at every level. To embark on this investigation of our members, in this context seems unwarranted and frankly, an unnecessary drain on the Commission's resources, which as stated earlier could be invested more productively elsewhere. While it may be fashionable in many quarters to speculate on police conduct and make accusations to suit the complainants needs at the



time, the Commission in the PAT's view should be deliberately circumspect and have proper foundation for pursuing such an investigation, which we do not accept is currently the case.

I refer specifically to the Executive Summary at page 4, final paragraph where it is stated that the Integrity Commission "could not conduct a survey of officers". This position is explained at paragraph [28] of the report by saying that without the PAT's support: "We decided that it would not be worthwhile to conduct the survey." The PAT believes that the Commission, contrary to the statement in the Executive Summary could have conducted its desired survey. Whether the survey would have elicited a sufficient response for its purposes would more likely, in the first instance, have relied on the perceived credibility of the Commission, rather than the PAT supporting the survey.

The President of the PAT is listed as having a 'special interest' in the report. The Commission sought this organisation's support regarding the proposed survey. The PAT expects that the Commission does not understand this organisation's role. Essentially the PAT exists to advance and protect the industrial, professional and welfare interests of its members. The PAT is not a branch of the Police Service, nor is it a government entity, it is a properly established industrial organisation. The Report and the associated investigation does not contribute to any of the PAT's objectives or responsibilities.

It does not enhance the police profession as it potentially confuses the boundaries around what is legitimate intelligence necessary for the proper performance of our members' sworn duty: *to cause the peace to be kept and preserved and prevent all offences against persons and properties in Tasmania*. Knowing who is connected or linked to whom, who lives at any given address, who uses a particular vehicle, are all legitimate avenues of inquiry that a police officer would exercise on a daily basis. Police are taught from the early stages of their careers, 'do not be a wondering police officer'. The knowledge about people in our community, town or city is what keeps us safe and allows police to effectively communicate with the people they come into contact with. Police understand this. Others, more often do not.

It does not advance the welfare of our members. Police officers are exposed to an array of traumatic and stressful situations. Often, they undertake their duty feeling isolated and without support. They are already under immense scrutiny in every aspect of their work with a continuing flow of persons and organisations prepared to criticise our members' performance and behaviour. As stated our members are already the most accountable group of workers in the State. To add another level of scrutiny by the Commission is counterproductive and further compromises their wellbeing.

Regarding Recommendation no. 1 the PAT believes its adoption is unjustified for police, largely proposing the same rationale we have expressed about the need for this investigation and the resultant report. There are sufficient safeguards and sanctions currently existing in an environment of heavy scrutiny and individual accountability.

The PAT's position is supported by the Commission's finding that "overall, Tasmania Police policies, practices and procedures are adequate and appropriate".

Yours sincerely

  
Pat Allen  
**PRESIDENT**





INTEGRITY  
COMMISSION

