Crime and Corruption Commission
QUEENSLAND

Operation Impala

Report on misuse of confidential information in the Queensland public sector

February 2020

Crime and Corruption Commission
QUEENSLAND

Operation Impala

Report on misuse of confidential information in the Queensland public sector

February 2020

ISBN: 978-1-876986-90-2

Crime and Corruption Commission

GPO Box 3123, Brisbane QLD 4001
Level 2, North Tower Green Square
515 St Pauls Terrace
Fortitude Valley QLD 4006

Phone: 07 3360 6060
(toll-free outside Brisbane: 1800 061 611)
Fax: 07 3360 6333
Email: mailbox@ccc.qld.gov.au

Note: This publication is accessible through the CCC website: www.ccc.qld.gov.au.

GPO Box 3123
Brisbane QLD 4001

Level 2
North Tower Green Square
515 St Pauls Terrace
Fortitude Valley QLD 4006

Tel.: **07 3360 6060**
Toll-free: 1800 061 611
(in Queensland outside Brisbane)

Fax: 07 3360 6333

mailbox@ccc.qld.gov.au
www.ccc.qld.gov.au

ABN 32 164 714 360

Crime and Corruption Commission
QUEENSLAND

February 2020

The Honourable Curtis Pitt MP
Speaker of the Legislative Assembly
Parliament House
George Street
BRISBANE QLD 4000

Dear Mr Speaker

In accordance with Section 69(1)(a) of the *Crime and Corruption Act 2001*, the Crime and Corruption Commission hereby furnishes to you its report – *Operation Impala – Report on misuse of confidential information in the Queensland public sector.*

Sincerely,

A J MacSporran QC
Chairperson

Contents

Abbreviations

ALRC	Australian Law Reform Commission
APPs	Australian Privacy Principles
CCC	Crime and Corruption Commission
CMC	Crime and Misconduct Commission
DoE	Department of Education
DoH	Department of Health
DTMR	Department of Transport and Main Roads
GCHHS	Gold Coast Hospital and Health Service
HHS	Hospital and Health Service
ICT	Information and Communications Technology
ieMR	Integrated Electronic Medical Record
IOMS	Integrated Offender Management System (database)
IPPs	Information Privacy Principles
IS	Information systems
Mackay HHS	Mackay Hospital and Health Service
MOU	Memorandum of Understanding
NPPs	National Privacy Principles
OAIC	Office of the Australian Information Commissioner
OIC	Office of the Information Commissioner (Queensland)
PbD	Privacy by Design
PSBA	Public Safety Business Agency
QCAT	Queensland Civil and Administrative Tribunal
QCS	Queensland Corrective Services
QGCIO	Queensland Government Chief Information Office
QGISCF	Queensland Government Information Security Classification Framework
QPRIME	Queensland Police Records and Information Management Exchange (database)
QPS	Queensland Police Service
TICA	Transport Integrated Customer Access (database)
TRAILS	Transport Registration and Integrated Licensing System (database)
UPA	Unit of public administration

Legislation

CC Act	*Crime and Corruption Act 2001*
CS Act	*Corrective Services Act 2006*
EGP Act	*Education (General Provisions) Act 2006*
HHB Act	*Hospital and Health Boards Act 2011*
HR Act	*Human Rights Act 2019*
IP Act	*Information Privacy Act 2009*
Privacy Act (Cth)	*Privacy Act 1988 (Cth)*
PSA Act	*Police Service Administration Act 1990*
RTI Act	*Right to Information Act 2009*
TI Act	*Transport Infrastructure Act 1994*
TPC Act	*Transport Planning and Coordination Act 1994*

Executive summary and recommendations

Overview

Improper access to and disclosure of confidential information by public sector employees has been one of the CCC's key areas of focus since 2016.

Operation Impala was a CCC corruption investigation authorised to examine the practices of a representative group of Queensland public sector agencies regarding their management of confidential information. During nine days of public hearings, Operation Impala identified the potential corruption risks associated with confidential information, as well as best-practice management principles and risk mitigation strategies. Agencies' experiences and insights have informed the CCC's 18 recommendations, which are designed to assist agencies strengthen their individual practices as well as improve consistency across the wider public sector. The CCC recommends a new criminal offence to deal with misuse of confidential information. It also recommends that some aspects of Queensland's privacy legislation be reformed to enable agencies to better detect and respond to misuse of confidential information, and to provide less complex and frustrating avenues of redress for people whose privacy has been breached.

Part 1: Operation Impala: scope and approach

The term "confidential information" is very broad. It can encompass commercially sensitive information such as that contained in contracts or tender documents and highly sensitive information relating to law enforcement methodology. However, the primary focus of Operation Impala was on unauthorised access to and disclosure of confidential information of a personal nature. This emphasis is in line with growing community expectations that people's personal information should be respected and kept private by any agency authorised to collect, store and use it. For this reason the use of the term "confidential information" in this report is a reference to confidential personal information.

This report outlines the current regulatory framework relating to confidential information and information privacy in Queensland, the roles and obligations of the State's public sector entities in the context of confidential information management, and the current trends in allegations of corrupt conduct associated with confidential information. For the purposes of Operation Impala, the CCC examined how seven public sector agencies — the Queensland Police Service, Queensland Corrective Services, the Department of Education, the Department of Transport and Main Roads, the Department of Health, Gold Coast Hospital and Health Service, and Mackay Hospital and Health Service — as a representative cross-section of the broader Queensland public sector are managing the confidential information they hold and their response to any misuse of it.

Part 2: Causes and consequences of misuse of information

Operation Impala examined the impacts of unauthorised access to and disclosure of information both on agencies and on the people whose information is accessed or disclosed to third parties without their knowledge or consent. It also sought agencies' views on why their staff continued to access information without legitimate reason to do so.

The main drivers of this behaviour were identified as personal interest (curiosity), the desire to obtain a material benefit, relationships that could make some employees more susceptible to misusing confidential information, and the personal circumstances of an individual.

The three most consistent risk areas contributing to employee misuse of confidential information were identified as:

- managing large volumes of information that is vastly diverse in nature
- ensuring consistent approaches to information security across devolved entities, and
- maintaining currency with advances in technology that have the potential to impact on information security, access control systems and or database usability.

Operation Impala found that the detrimental effects on agencies from the misuse of confidential information included financial liability for the actions of their employees as well as adverse community perceptions of the Queensland public sector. The hearings also detailed the significant personal consequences on victims of misuse of confidential information. Such misuse was found to have ongoing and long-lasting effects including stress, feelings of vulnerability, financial loss, and frustration with the difficulty of obtaining redress or adequate compensation.

Part 3: Agency frameworks for managing confidential information

The CCC considered agencies' frameworks for managing confidential information, having regard to the "Privacy by Design" (PbD) approach that is seen by many as the global standard to assure privacy protection, and the varying degree of effectiveness across the agencies.

The frameworks comprised organisational systems of technical controls such as IT protocols and security regimes supported by promotion of an effective information privacy culture. Agencies described their use of organisational information controls and management strategies such as authentication and authorisation, passwords, user accounts access review processes and tailored access controls for people classified as "vulnerable". Significantly, vulnerable people — including domestic and family violence victims and high-profile individuals — were identified as being at particular risk of having their information misused when accessing government services. Six of the seven subject agencies agreed that organisational systems could be reviewed and refined to cater more specifically to the needs of vulnerable people, in order to ensure earlier detection of (actual or potential) information misuse.[1] In addition, improved prevention and detection strategies should be integrated into agency databases to afford further protection.

Agency responses to misuse of confidential information need to be simple and precise, in order to accurately convey the intended messages to staff and to ensure they are understood. An effective deterrent message must be based on consequences and sanctions that reflect the seriousness of offending. Developing and maintaining an effective information privacy culture relies on the adequacy of internal policies, education and awareness campaigns, and practical training. The use of de-identified case studies was found to be a very useful educative and training tool, as they provided real-life scenarios that helped staff interpret the intention of policies. A common issue identified was decentralisation and the challenges it created for lead agencies in guiding and monitoring their smaller devolved entities.

Operation Impala identified inconsistent approaches to dealing with allegations regarding misuse of confidential information. To maintain public confidence, agencies need to deal with misuse of confidential information in a way that is consistent, efficient and appropriate. The seven subject agencies experienced challenges when determining whether to deal with an allegation in the disciplinary or criminal arena, and in deciding when to refer matters to the police for criminal investigation. Some of the other challenges for public sector agencies in responding to misuse of confidential information were ensuring consistent disciplinary outcomes (and communicating the reasons for those outcomes) and minimising the risks associated with initiating disciplinary proceedings before matters were referred to the police for consideration of criminal investigation.

1 DTMR's response to a draft of this report stated that "TMR has a mature customer records suppression policy in place …".

The CCC is recommending a range of technical and organisational enhancements (**Recommendations 1–9** and **18**) to strengthen agencies' information management systems and create a more privacy-aware culture.

To assist agencies determine the seriousness of an incident involving confidential information, the CCC has developed a flowchart to assist agencies to deal with allegations more efficiently and consistently, improve employee understanding, reduce the incidence of breaches and mitigate (new or ongoing) risk.

Part 4: Legislative reform

As a result of Operation Impala, the CCC is recommending legislative reform.

It is recommending the creation of a new offence in the Criminal Code that will be more useful in prosecuting offending related to misuse of confidential information (**Recommendation 10**) and obviate the challenges of trying to prosecute misuse under the existing criminal offence (s. 408E Computer Hacking and Misuse). The CCC also recommends that further remedial avenues be made available for victims of misuse of confidential information (**Recommendations 13, 15** and **17**). It is hoped that the proposed extension and clarification of the Information Commissioner's privacy powers and practices (**Recommendations 11, 12, 14** and **15**), in addition to strengthening and clarifying protections to victims under Queensland's privacy legislation, will generate and make more accessible other redress options for victims of misuse of confidential information. Queensland's new human rights legislation will also make available further avenues of recourse for victims, which is expected to complement the proposed refinement of the existing privacy principles, having regard to the national counterpart principles (**Recommendation 16**).

The CCC is also recommending a new tort for privacy, to be located in Queensland legislation (**Recommendation 17**). The creation of a statutory tort (as opposed to one developing at common law) is preferred, as it provides clearer guidance for satisfaction of carefully selected elements, it may be more flexibly developed, and might provide for a greater range of remedies not necessarily available under privacy legislation.

Recommendations

Recommendation 1 – Access control mechanisms

That agencies:

1. ensure all computer databases where confidential information is stored have unique user identifications log-ons
2. conduct quarterly user access reviews and monitoring of user access changes to help prevent and minimise unauthorised use of these databases
3. ensure additional access control mechanisms are implemented on confidential information of vulnerable people.

Recommendation 2 – Audit responsibility when sharing data

That public sector agencies ensure MOUs or other agreements which set out the processes and roles in relation to data sharing between agencies contain clauses that specify:

1. which agency is responsible for conducting targeted audits of shared data
2. regularly defined intervals at which audits are to be conducted, preferably quarterly.

Recommendation 3 – ICT Information Access policy

3.1 That all public sector agencies develop a comprehensive and concise ICT Information Access policy. The policy should refer to the Criminal Code, the relevant public sector agency governing Act and the Information Privacy Act. It is critical that language used is standardised to ensure consistency and better understanding. In particular the policy should include for each of these three Acts:

1. the meaning of confidential information
2. the meaning of unauthorised use
3. the meaning of unauthorised disclosure
4. the range of potential sanctions including criminal charges and disciplinary proceedings, such as termination, demotion, and/or the imposition of a post-separation declaration, and
5. de-identified case studies of substantiated allegations relating to the misuse of confidential information and the consequences of those matters for the employee.

3.2 That public sector agencies with decentralised agencies (for example, Queensland Health and the Department of Education) provide sufficient support to ensure that the decentralised agencies have comprehensive and concise ICT Information Access policies in place. Sufficient support includes, but is not limited to:

1. providing templates and
2. Reviewing the policies implemented by decentralised agencies annually.

Recommendation 4 – Confidential information access and privacy training

4.1 That agencies ensure that training:

1. is developed and provided to all public sector employees prior to gaining access to any database that contains confidential information
2. is developed and provided annually to all public sector employees who have access to confidential information
3. reflects the respective ICT access and use policy, including references to the Criminal Code, the relevant public sector agency governing Act and the Information Privacy Act. The language used in the training material should be consistent and include explanation of items numbered 1 to 5 outlined in Recommendation 3.1
4. comprises a combination of online, face-to-face and video modules
5. records of the content and participation by employees are kept
6. is assessed annually to determine levels of retention and understanding of the content of the respective Information Privacy policy and supporting training material.

4.2 That public sector agencies with decentralised workforces (for example, Queensland Health and the Department of Education) provide sufficient support to ensure that the decentralised agencies conduct all-inclusive training. Sufficient support includes, but is not limited to:

1. providing guidelines, and
2. conducting an annual review of the decentralised agencies' training.

Recommendation 5 – Privacy awareness messaging

That public sector agencies undertake regular information privacy awareness campaigns including but not limited to:

1. annual email messaging to all employees by the Commissioner, Director-General or Chief Executive Officer to communicate the agency's position clearly as regards information privacy, including acceptable and unacceptable conduct
2. bi-annual email messaging of same to employees by senior executive officers
3. screensavers and posters that stipulate the consequences of misusing a restricted computer database [see items 1 to 5 of Recommendation 3.1], to be updated on a quarterly basis
4. log-on warnings displayed before accessing a restricted computer database to remind public sector employees that access is logged and monitored and that consequences of misuse of confidential information may result in criminal charges under s. 408E of the Criminal Code and/or disciplinary sanctions, and
5. de-identified case studies—for example, for inclusion in monthly newsletters or for discussion during toolbox talks.

Recommendation 6 – Dealing with misuse of confidential information

That public sector agencies:

1. Consider criminal prosecution upon detection of misuse of confidential information by public sector employees, which generally will require the matter be referred to the QPS as a criminal complaint in the first instance prior to a determination being made with respect to the instigation of disciplinary proceedings.
2. Apply and adapt, if necessary, the CCC's assessment flowchart to ensure consistency in decision-making processes with respect to incidences of misuse of confidential information, including the decision to refer to the QPS and the decision to institute disciplinary proceedings. Public sector agencies are to retain contemporaneous records to justify decisions made.
3. Pursue post-separation disciplinary proceedings where appropriate.

Recommendation 7 – Referral for criminal proceedings

That the QPS:

1. Manage all complaints of misuse of confidential information by public sector employees through the central QPS unit in the first instance.
2. Provide clear and cogent advice to agencies in relation to the reasons for not commencing criminal prosecutions when matters are referred from the agency.
3. Provide a template and guidelines for public sector agencies to refer a suspected criminal with respect to misuse of confidential information to assist with the compilation of relevant information for the QPS to use during the determination to commence an investigation.

Recommendation 8 – Improved prevention and detection systems

That public sector agencies are to:

1. Develop and define additional protections to safeguard confidential information that relates to vulnerable including high profile persons. Public sector agencies should develop their own categories of vulnerable persons. Protections should be proportional to ensure that operational efficiency is not compromised and should include:
   - flags when records of vulnerable or high profile persons have been accessed; and
   - targeted quarterly audits of the flags.
2. Conduct quarterly targeted audits of access logs to identify possible misuses of confidential information. Agencies are to develop their own categories for the targeted audits, based on a risk assessment.
3. Develop systems that monitor outbound emails, after hours and remote accesses; as well as the deployment of data analytics to report unusual accesses. That the Queensland Government Chief Information Officer (QGCIO) advise agencies with respect to proposed improved proactive auditing systems.

Recommendation 9 – QHealth

That the Department of Health provide assistance to all Hospital and Health Services to remove the backlogs of potential breaches of the eMR and ieMR databases detected by the P2Sentinel software.

Recommendation 10 – A new criminal offence

That the Criminal Code be amended to add a new offence of **misuse of confidential information by public officers**, to contain the following attributes:

1. Be divided into two parts, one relating specifically to misuse of confidential information on a computer and the other to provide for an offence misuse of any confidential information regardless of its source.
2. Access to the information is an offence where it was not in furtherance of the performance of a function of the agency.
3. The simpliciter offence which involves only access to the confidential information is to be a crime, punishable by 5 years imprisonment.
4. There are to be three aggravating circumstances to the simpliciter offence where the term of imprisonment increases to 10 years, namely:
   a. where the public officer or another person obtains a benefit, or
   b. when disclosure is made to a third party, or
   c. where access could facilitate the commission of a crime.
5. It is to be a defence if the access to the information was authorised, justified or excused by law.
6. The offence is to be added to the list of the indictable offences under s. 552A (1)(a) which must be heard and decided summarily on prosecution election.
7. The offence is to contain the following definition section:

   benefit includes:

   (i) obtaining knowledge of information from a database, or
   (ii) finding that there is no record in the database, or
   (iii) obtaining knowledge of information that is available from another public source

computer includes any electronic device for storing or processing information

confidential information includes all data, files and documents, irrespective of whether the information is publicly available from another source. The focus should be on the source of the information obtained as opposed to whether it could have been obtained lawfully via some other means.

Recommendation 11 – Central enquiry service

That OIC strengthens its enquiry service for victims who have had their confidential information misused, to include if accepted services outlined in recommendations 12, 14 and 15. Such services should include telephone and face-to-face advice delivery, with information available online, and scope to make referrals to other relevant agencies.

Recommendation 12 – Mandatory Notification Scheme

That a mandatory data breach notification scheme be implemented in Queensland and that the OIC be responsible for developing the scheme, and receiving and managing the notifications.

Recommendation 13 – Updates to complainants regarding confidential information misuse complaints

That public sector agencies provide three-monthly updates to complainants regarding the management of their complaint, with sufficient details, where appropriate, regarding the progress and final outcome.

Recommendation 14 – Own-motion powers for the OIC

That the OIC have:

1. own-motion powers under the IP Act to strengthen existing powers and better identify systemic issues arising from an act or practice of an agency.
2. the power to make a declaration following an own-motion investigation, to be modelled on the comparable Commonwealth provisions.

Recommendation 15 – Extending the role of the OIC in proceedings

That the OIC be able to appear as a friend of the court (*amicus curiae)*, and have the power to intervene in QCAT proceedings, where appropriate and with leave of the court.

Recommendation 16 – A single set of privacy principles

That the IPPs and NPPs in the IP Act be amalgamated and strengthened, having regard to the APPs contained in the Privacy Act (Cth); and in particular the:

1. definition of "reasonable steps" in the fourth of each set of principles relating to security of data be further defined in accordance with the terms of Article 32 of the EU GDPR; and
2. definition of "personal information" be amended in the IP Act to accord with the current version contained in the Privacy Act (Cth).

Recommendation 17 – Statutory tort for misuse of private information

That the Queensland Government consider the introduction of a statutory tort for serious invasion of privacy by the misuse of private information, such as by collecting or disclosing private information about the plaintiff, as described in the ALRC 2014 Report.

Recommendation 18 – Privacy Champion

That a "privacy champion" be embedded in agencies at a senior officer level, with the view to incorporating PbD into executive decision-making processes.

Part 1 – The privacy landscape in Queensland

Part 1 establishes the background and key concepts to be discussed in the report.

Chapter 1 looks at the value of information and importance of safeguarding it. It defines the term "confidential information" as used in this report, and examines related concepts of data/information security and breaches of privacy. Because the management of confidential information and the action to be taken once a breach is identified (which may include criminal prosecution) is carried out by different agencies, the chapter provides an overview of the regulatory framework and the roles of different Queensland agencies in this regard.

Chapter 2 discusses the role of the CCC and why it determined to undertake Operation Impala.

Chapter 3 describes the types and value of information collected and managed by public sector agencies, and explains why the CCC selected the seven agencies to be examined as part of Operation Impala.

Chapter 1 — Confidential information: its value and management

Definition and scope

The term "confidential information" is quite broad and could comprise a wide range of information including personal information, commercially sensitive information such as contracts or tender documents, and any other data, files or documents stored on a restricted computer database. When allegations are received by the CCC regarding corrupt conduct, they are categorised based on the type of conduct. For the purpose of Operation Impala, conduct which is classified as "Misuse of confidential information" was used to examine relevant allegations which had been reported to the CCC.

Operation Impala further focused on confidential information held by agencies which was of a personal nature about members of the public and involved unauthorised access and disclosure of personal information[2] about members of the public, by public sector employees. For this reason, the report refers to "confidential information" when describing the types of information accessed or disclosed by public sector employees.

It is acknowledged that misuse of confidential information can also occur due to unintentional errors or oversights by employees. For instance, misuse of information may be inadvertent or unintentional when a storage device is misplaced or an employee incorrectly addresses an email to the wrong recipient. These types of misuse of confidential information, although potentially serious, were not the focus of Operation Impala.

The value of information

Data, both current and historical — including people's personal details such as residential addresses, phone numbers and emails, court orders, information about children, medical information and financial information—is an increasingly valuable commodity. It is collected by both government agencies and private companies for a variety of uses in the delivery of public services and for legitimate commercial enterprises. Citizens are regularly asked to, and agree to, provide their personal information to government as part of the social contract for the provision of services and, in some instances, government agencies may use statutory powers to collect information without the consent of the public.

This data may also be sought and exploited by commercial enterprises seeking market advantage or an extended consumer base, or even stolen or appropriated for use in criminal activity such as identity fraud and cybercrime. Data theft and breaches of information privacy are now a global concern for government, legitimate private-sector operations, and the people whose information is being improperly accessed and/or disclosed.

For this reason, an increasing range of legislation and other safeguards, warnings and management requirements are being put around the collection, storage and use of confidential data.

At times, confidential information is also accessed and used by employees of government agencies for purposes not related to their work. This report examines the reasons why employees of

2 Personal information is defined under s. 12 of the *Information Privacy Act 2009*. It includes information or an opinion forming part of a database, whether true or not, and whether or not recorded in a material form, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

government agencies improperly access this confidential information, and what controls and protections agencies have in place or require to protect this data; it then examines how agencies should deal with breaches of information and discusses a number of areas for reform to improve agency responses and outcomes for victims.

Government data holdings

Across the public sector, unauthorised access to and misuse of information systems and datasets pose a significant threat. The threat looms largest for agencies that record some of the most sensitive — and therefore valuable and highly sought after — personal information, for example, contact details, health records, criminal histories and intelligence. With the transfer of confidential information from paper-based storage and management systems to electronic systems over the last decade making it easier to access extensive data holdings no matter where they are located, concern around breaches of information privacy has increased.[3]

Privacy and data breaches have serious consequences. They can adversely affect the ability of government agencies to undertake their functions. When this type of conduct becomes publicly known, it reduces public confidence in the integrity of government operations.

However, of greater concern is the impact such a breach can have on the person whose information has been accessed and possibly disclosed to other parties who have no lawful right to that knowledge. In some cases, a breach of privacy can pose a serious risk to their or another's safety. Misuse of information can also cause significant and irreparable harm to people whose personal information is disclosed, including (but not limited to) embarrassment, distress, physical harm, reputational damage, financial loss and reduced mental wellbeing.[4] For this reason, any misuse of information entrusted to public sector agencies involves a serious breach of trust. At its highest, it is a criminal offence.

The regulatory framework in Queensland

Given the importance of managing and protecting confidential information, the remainder of this chapter outlines the oversight bodies, legislation and controls currently in place in Queensland to ensure that its citizens' information is collected, stored, managed and released appropriately. It also describes the current regime in place in relation to notification of breaches, and the rights of victims of breaches and the recourse open to them.

Office of the Information Commissioner

The Office of the Information Commissioner (OIC) is an independent statutory body that reports to the Queensland Parliament. OIC has a statutory role under the *Right to Information Act 2009* and the *Information Privacy Act 2009* to facilitate greater and easier access to information held by government agencies. OIC also assists agencies to understand their obligations under the IP Act to safeguard personal information that they hold.

OIC's statutory functions include mediating privacy complaints against Queensland government agencies, issuing guidelines on privacy best practice, initiating privacy education and training, and conducting audits and reviews to monitor agency performance and compliance with the RTI Act and

3 Rajakaruna, N., Henry, P. J., & Scott, A. J. (2019). Misuse of Police Information Systems: Predicting Perceived Likelihood of Misuse among Unsworn Police Employees. *Policing: A Journal of Policy and Practice*, p. 1

4 de Vries, Kevin. (2019). Privacy, confidentiality and health information. *Australian Journal of Pharmacy*, May 2019, p. 79. Accessed from https://ajp.com.au/cpd-activities/privacy-confidentiality-and-health-information/

the IP Act. OIC reviews decisions of agencies and Ministers on access to and amendment of information under the RTI and IP Act.

Privacy Commissioner

The Privacy Commissioner supports the Information Commissioner in performing the above-mentioned functions. The Privacy Commissioner leads the privacy complaint and advice functions, including providing privacy impact assessments of key policy and project proposals, such as information sharing or adoption of technology. The Privacy Commissioner also leads the annual Privacy Awareness Week Campaign.

Information Privacy Act 2009

The Information Privacy Act recognises the importance of protecting the personal information of members of the public. It creates a right for members of the public to access and amend their own personal information and provides rules or "privacy principles" that give guidance on how Queensland government agencies collect, store, use and disclose personal information.

There are 11 information privacy principles (IPPs) (schedule 3) that pertain to all agencies, except health; and nine national privacy principles (NPPs) (schedule 4) that safeguard the handling of personal information in health agencies.

The NPPs[5] set out how personal information must be collected and managed for public health sector agencies. While not identical to the NPPs, the Australian Privacy Principles (APPs) contain a very similar list of obligations under Commonwealth legislation. The relationship between these principles is discussed later in the report in the context of potential improvements to the regulatory regime in Queensland.

One of the IPPs that will be discussed in more detail is IPP4 - Storage and security of personal information. It requires relevant agencies to manage personal information in an open and transparent way, which includes taking reasonable steps to implement systems, practices and procedures in a way that will ensure compliance with the stated principles.

Queensland Government Chief Information Officer

The Queensland Government Chief Information Officer (QGCIO) is responsible for ensuring the government's ICT investments support policy outcomes that are reliable, focused on service delivery to the community and represent value for money. The QGCIO provides advice to Queensland government agencies and executive government on issues such as:

- setting ICT strategy, policies and standards
- adopting better practice for ICT investment management
- identifying and managing risks, including "over the horizon" risks
- developing proposals for major whole-of-government investments
- identifying and managing strategic workforce capability issues
- improving contract outcomes, and
- facilitating strategic relationships with industry partners.

As such, the QGCIO is in a position to provide guidance in relation to best practice for systems and standards to protect confidential information from improper access and use.

---

5 The NPPs were originally introduced by the *Privacy Act 1988* (Cth) and applied to a number of organisations including State health agencies. In 2014 the NPPs were replaced by the Australian Privacy Principles (APPs), however the same amendments have not been made at the State level.

The QGCIO has produced standards and guidelines, including:

- IS18:2018 – Information security policy. This policy seeks to ensure all agencies apply a consistent, risk-based approach to the implementation of information security to maintain confidentiality, integrity and availability.
- IS33 – Information access and use policy. This policy relates to information sharing.
- QGISCF – Information Security Classification Framework. Agencies should classify their information and assets according to business impact and implement appropriate controls according to the classification. The Confidentiality labels are official (low or negligible confidentiality impact), sensitive (moderate confidentiality impact) and protected (high confidentiality impact).

Human Rights Commission

Since 1 January 2020 Queensland has enshrined privacy as one of the 23 fundamental human rights, which requires relevant agencies to ensure that decisions and actions are consistent with these rights. Section 25 of the HR Act provides that:

> *A person has the right to not have their privacy (or the privacy of their family, home or correspondence) unlawfully or arbitrarily interfered with, and has the right to not have their reputation unlawfully attacked*

Agencies to whom the HR Act applies must ensure that they give proper consideration to the HR Act when making decisions which may interfere with a person's privacy as outlined in section 25.

Agency-specific legislation

Each public sector agency has its own specific legislation that places limits on disclosure of the information it holds and imposes penalties for disclosure of confidential information other than as permitted by that legislation. Confidentiality provisions apply to employees who have come across confidential information in the course of their employment in order to carry out the agency's functions. These provisions are designed to place limitations on the circumstances and the persons to whom this information can be lawfully disclosed. They are not necessarily intended to govern circumstances in which employees access information for purposes not connected with the performance of their functions. For this reason they are not by themselves a sufficient protection in relation to confidential information.

Criminal Code

Several offences in the Criminal Code relate to improper access and/or disclosure of confidential information. The most relevant to Operation Impala is s. 408E – Computer Hacking and Misuse (discussed in more detail in chapter 10).

Victim rights and recourse

In Queensland, under the present framework, agencies are not required by law to automatically notify people that their confidential information has been accessed.

When a person discovers that their information has been accessed or disclosed to someone else, they can lodge a complaint with the agency involved, the QPS or the CCC. Where the complainant is not satisfied with the agency's response, they can make their complaint to the OIC,

They may bring an action in the Queensland Civil and Administrative Tribunal (QCAT) or commence their own proceeding in court, however this can be time-consuming and costly. The courses of action available to victims of misuse of confidential information, as well as recommendations for improvement to the current system, are discussed in chapter 11.

Best-practice principles and approaches

In addition to the regulatory framework outlined above, a growing body of best-practice principles and approaches to information privacy and the management of confidential information is being developed. This includes the APPs and Privacy by Design (PbD), which is seen by many as the global standard by which to construct privacy protection (see chapter 12).

Corrupt conduct and misconduct

When a public sector employee improperly accesses confidential information held by a government agency, in circumstances where that would be a criminal offence or warrant their dismissal, that conduct may be corrupt conduct. Under the *Crime and Corruption Act 2001,* Government agencies, including the QPS, have an obligation to report suspected corruption[6] to the CCC.

Under the current legislation in Queensland, the only circumstance in which government agencies must report a breach of privacy is when it could also amount to corrupt conduct. As outlined above, this means that victims of misuse of confidential information may not always be notified of the breach by the agency involved, a significant gap in the current system and one which may require legislative action.

The CCC found evidence that misuse of confidential information was significantly under-reported and often went undetected (see chapter 9). Evidence of this, which is discussed later in the report, includes:

- significant increases in reporting of allegations of corrupt conduct following the introduction by agencies of audits, for example, P2Sentinel with HHSs (Chapter 9)
- significant increases in reporting following an increase in focus on misuse of confidential information by an agency, for example, QCS following Taskforce Flaxton (Chapter 3), and
- a significant increase (over 700%) in reporting of data breaches, at the Commonwealth level, following the introduction of a mandatory reporting scheme (Chapter 11).

For this reason the CCC examined what protection and detection mechanisms government agencies currently have in place, or should aim to introduce, to safeguard the confidential information they hold and minimise the corruption risks associated with that information.

6 Corruption includes both corrupt conduct and police misconduct.

Chapter 2 — Operation Impala

The misuse of confidential information – either through unauthorised access and/or unauthorised disclosure – has been a longstanding issue in the Queensland public sector. Such misuse of information can be a key enabler of other types of corrupt conduct.[7] For this reason, improper access to and disclosure of confidential information is an area of significant corruption risk and has been one of the CCC's key areas of focus since 2016.

Allegations of corrupt conduct related to confidential information

Table 1 shows that the number of allegations relating to misuse of confidential information across the public sector increased from 713 in 2015-16 to 1060 in 2018-19. This represents an increase of almost 50 per cent over a three-year period. Those 1060 allegations[8] represented 13 per cent of all allegations of corrupt conduct received in that financial year.

Table 1: Misuse of confidential information: complaints and allegations[9]

Year	No. of complaints[10]	No. of allegations
2018-19	603	1060
2017-18	492	762
2016-17	459	710
2015-16	438	713

The CCC began Operation Impala in September 2019 with a view to strengthening transparency, integrity and accountability in the Queensland public sector. Specifically, it was designed to examine:

1. Factors which facilitate misuse of information within the Queensland public sector, by examination of the technical, people, and systems components of information management within the following identified agencies – Queensland Police Service, Queensland Corrective Services, Department of Education, Department of Health (including selected Hospital and Health Services) and Department of Transport and Main Roads.
2. Features of the legislative, policy and operational environment within each agency that may enable corrupt conduct to occur or are vulnerable to corrupt conduct.
3. Reforms to better prevent, detect and deal with corrupt conduct relating to misuse of information within the identified agencies, and lessons that can be extrapolated to the broader Queensland public sector.

7 IBAC. (2019). *Unauthorised access and disclosure of information held by Victoria Police: An analysis of corruption risks and prevention opportunities*, p. 5. Accessed from https://www.ibac.vic.gov.au/publications-and-resources/article/unauthorised-access-and-disclosure-of-information-held-by-victoria-police

8 See *CCC Annual Report 2018-19*, p. 41. Accessed from https://www.ccc.qld.gov.au/sites/default/files/Docs/Publications/CCC/CCC-Annual-Report-2018-19.pdf

9 Data from the CCC's complaints management database (COMPASS).

10 A single complaint may contain multiple allegations.

CCC jurisdiction

The CCC has a number of functions including to investigate corrupt conduct, particularly more serious cases of corrupt conduct[11], prevent corruption[12] and raise the standards of integrity and conduct in units of public administration.[13] Further, the CCC has an overriding responsibility to promote public confidence in the integrity of UPAs.[14] These key responsibilities guided the focus of Operation Impala.

Corruption

Corruption is defined in the CC Act to include both corrupt conduct and police misconduct. In relation to the QPS, the CCC has an expanded jurisdiction, which is greater than other government agencies, to examine and investigate not only allegations of corrupt conduct, but also police misconduct.[15]

The CC Act defines corrupt conduct as conduct by a person that:

- adversely affects, or could adversely affect, directly or indirectly, the performance of functions or the exercise of powers of—
  - a unit of public administration; or
  - a person holding an appointment; and
- results, or could result, directly or indirectly, in the performance of functions or the exercise of powers mentioned above in a way that—
  - is not honest or is not impartial; or
  - involves a breach of the trust placed in a person holding an appointment, either knowingly or recklessly; or
  - involves a misuse of information or material acquired in or in connection with the performance of functions or the exercise of powers of a person holding an appointment; and
- would, if proved, be a criminal offence; or a dismissible disciplinary breach.

From 1 March 2019 the definition of corrupt conduct was expanded to include conduct by a person that:

- impairs, or could impair, public confidence in public administration; and
- involves, or could involve, any of the following—
  - collusive tendering:
  - fraud relating to an application for a license, permit or other authority under an Act with a purpose or object of any of the following (however described)—
    - protecting health or safety of persons;
    - protecting the environment;
    - protecting or managing the use of the State's natural, cultural, mining or energy resources;
  - dishonestly obtaining, or helping someone to dishonestly obtain, a benefit from the payment or application of public funds or the disposition of State assets;
  - evading a State tax, levy or duty or otherwise fraudulently causing a loss of State revenue;

11 CC Act, s. 5(3)

12 CC Act, s. 23

13 CC Act, s. 33(1)(a)

14 CC Act, s. 34(d)

15 Police misconduct is defined in schedule 2 of the CC Act.

- fraudulently obtaining or retaining an appointment; and
- would, if proved, be —
  - a criminal offence; or
  - a disciplinary breach providing reasonable grounds for terminating the person's services, if the person is or were the holder of an appointment.

Misuse of confidential information such as unauthorised access and disclosure can amount to corrupt conduct under the CC Act.

Approach

Selection of agencies

The focus of Operation Impala was on issues related to misuse of confidential information rather than on the conduct of particular agencies. The CCC did none the less select seven agencies to be examined as part of Operation Impala, based on a number of factors including:

- the type of data they held
- the number and type of allegations of corrupt conduct that had been reported to the CCC in relation to misuse of confidential information, and
- the approach that agencies had adopted in relation to detection of these types of allegations.

The agencies were selected to obtain a representative sample of the types of issues which are reported to the CCC regarding misuse of confidential information by employees across the public sector.

As a result, this report is not intended to be a report card on the performance of the seven agencies and how they have dealt with allegations of misuse of confidential information.

Where case studies involving particular agencies have been included or referred to, or the evidence of officers from those agencies has been quoted, the CCC's aim is to put particular issues in context and to explain how and why improvements can be made across the entire public sector.

Examination of information holdings and databases

Data provided in response to an initial request for information from the seven subject agencies showed that their information systems held many different kinds of confidential information, not all of which was of a personal nature. Accordingly, the CCC selected to analyse only those agency information systems that held the most valuable confidential information. The following agency databases were selected:

- QPS: QPRIME
- QCS: IOMS
- DTMR: TRAILS/TICA
- DoE: OneSchool
- DoH: ieMR
- GCHHS: ieMR
- Mackay HHS: ieMR.

Public hearing

On 9 August 2019, the CCC announced it would hold a public hearing in relation to Operation Impala (see Appendix 1 for the terms of reference).[16] In arriving at this decision, the CCC considered:

- the issues which the hearing could explore to determine the maturity level of each agency in relation to their capacity to effectively safeguard confidential information from unauthorised access and disclosure
- the need to promote transparency, integrity and accountability to ensure that all UPAs are employing or working towards the implementation of systems and practices regarded as best practice, and
- the CCC's function to raise standards of integrity in UPAs and its overriding responsibility to promote public confidence.

The CCC resolved that these functions and responsibilities could not be achieved by private hearings and that closing the hearing would be contrary to the public interest.[17]

The public hearing was held from 11 to 22 November 2019. It heard evidence from 31 witnesses, including:

- Mr Philip Green, Queensland Privacy Commissioner
- Ms Rachael Rangihaeata, Queensland Information Commissioner
- Mr Scott McDougall, Queensland Human Rights Commissioner
- Mr Andrew Mills, Queensland Government Chief Information Officer
- Sixteen representatives from the seven agencies, including their Directors-General and Commissioners, where applicable
- Four representatives from key stakeholders, including the Victorian Police Service, Public Safety Business Agency, the Domestic Violence Prevention Centre, and an independent social justice advocate
- One representative each from the Queensland Police Union of Employees (QPUE), the Queensland Nurses and Midwives' Union, and the Queensland Teachers' Union
- Four subject area experts.

A full list of the witnesses who appeared at the hearing can be found at Appendix 2. The public hearing was live-streamed. Archives of the live-stream, transcripts and exhibits from the hearing can be found on the CCC's website.[18]

One witness gave evidence in a closed hearing (that is, it was not open for members of the public to attend and it was not streamed on the CCC's website). The witness had her confidential information misused by a QPS officer, Neil Punchard (see pages 42-43). The witness initially contacted the CCC to provide a submission and communicated a desire to assist the CCC with this inquiry by providing further relevant information regarding the impact of the misuse. The CCC determined to call the witness to the hearing, but closed the hearing in order to protect her identity. In consultation with the witness, a redacted copy of her evidence has been made available on the CCC's website.

16 Pursuant to ss. 176 and 177(2) (c)(ii) of the CC Act, the Commission authorised and approved the holding of public hearings in relation to Operation Impala. Under ss. 176 and 177, the CCC has the authority to hold public hearings in relation to any matter relevant to the performance of its functions, if it considers that closing the hearing to the public would be contrary to the public interest.

17 CC Act, s. 177(2)(i)

18 See www.ccc.qld.gov.au/public-hearings/operation-impala

Call for public submissions

On 20 September 2019, the CCC called for written submissions to Operation Impala, inviting key stakeholders and members of the public to contribute their views regarding improper access to and disclosure of confidential information, and the associated corruption risks in the Queensland public sector. As part of the call for submissions, an issues paper providing background information and key questions to guide written submissions was made available on the CCC's website. The submission period closed on 9 October 2019. In total, the CCC received 11 submissions, 10 of which were published on the CCC's website (one confidential submission was not published).

Case studies

As part of Operation Impala, the CCC also analysed cases from the subject agencies in order to understand:

- the types of information being improperly accessed and or disseminated
- where possible, the reasons for the improper access and or dissemination
- the databases where the breaches were being detected
- the types of sanctions that were being imposed in relation to substantiated allegations
- the frequency with which allegations were being reported to the QPS and, if not being reported, the reasons why.

Other sources of information

The CCC also analysed a range of other information including:

- CCC allegations data relating to the misuse of confidential information
- data, policies, procedures and reports from the subject agencies
- relevant legislation, reports and academic literature from Queensland and interstate.

Consultation – procedural fairness

Under the CC Act, the CCC must act independently, impartially and fairly, having regard to the purposes of the CC Act and the importance of protecting the public interest.19 The CCC must also act in accordance with the HR Act and must not act or make a decision in a way that is not compatible with human rights or, in making a decision, fail to give proper consideration to a human right relevant to the decision.20 The CCC acknowledges the publication of this report is likely to engage human rights in relation to privacy and reputation. Having regard to the clear statutory basis and reasons for the publication of this report, together with the measures adopted to ensure fairness with respect to the content of the report, the CCC considers the decision to publish the report is compatible with human rights.

For the purpose of procedural fairness[21], the CCC gave the draft report (or relevant parts of it) to people and organisations referred to in it (whether those people or organisations were specifically identified or not) and invited them to make submissions prior to the CCC determining the final form of the report. Respondents could provide confidential or non-confidential submissions. The CCC indicated to respondents that non-confidential submissions might be annexed to the final report, while confidential submissions would be noted as received but not attached to the final report.

19 CC Act, s. 57

20 HR Act, s. 58

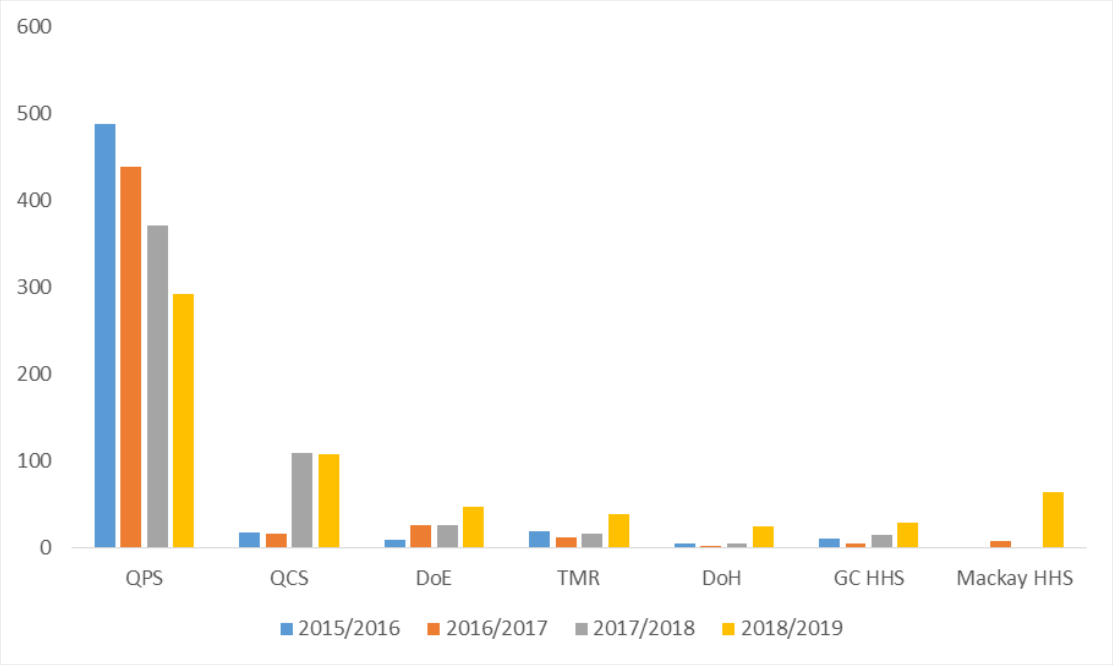
21 CC Act, s. 71A

The CCC determined not to annex any submissions to the report as it was considered that to the extent that any submissions are not reflected in the report the content is not adverse about the organisation or individual.

Chapter 3 — Subject agencies

Operation Impala focused on the misuse of confidential information in seven Queensland public sector agencies. Analysis of CCC's internal data shows that the selected agencies record a significant number of complaints and allegations relating to misuse of confidential information, as shown in figure 1. They also hold some of the most valuable confidential information such as people's health records and contact details, criminal intelligence and the like.

Figure 1: Allegations regarding misuse of confidential information (July 2015-June 2019)[22]



Source: *Crime and Corruption Commission*

The CCC notes that the increase in allegations, for some agencies, which is represented in figure 1 may be attributed a number of different factors including:

- an increased focus by agencies on improving awareness that this type of conduct is unacceptable leading to an increase in reporting
- an increase in the frequency or scope of audits, or
- improved detection systems.

The increase in allegations do not necessarily reflect an increase in improper behaviour by employees.

The CCC also notes that there are limitations to the interpretation of allegation data, including that:

- the matters may, after investigation, turn out to be unsubstantiated
- allegations may be vague and lacking completeness in their details, and
- allegations data only indicate perceptions of corruption, and do not necessarily reflect poor culture or a lack of prevention practices.

22 QPS data includes police misconduct allegations. Under s. 37 of the CC Act, the Commissioner of Police has a duty to notify the CCC of police misconduct. Also DoH data excludes Queensland Ambulance Services and HHSs.

Queensland Police Service

The Queensland Police Service (QPS) performs a variety of diverse functions which are outlined in the Police Service Administration Act (PSA Act). Under section 2.3 of the PSA Act, the QPS is responsible for a range of functions including:

- preserving peace and good order in all areas of Queensland
- protecting and supporting the Queensland community
- preventing and detecting crime
- upholding the law
- administering the law fairly and efficiently
- bringing offenders to justice.[23]

Essential to the performance of the QPS' functions is the collection and examination of a wide variety of information from various sources.[24] A valuable source of information for the QPS is the public. It is essential that the public have confidence that the officers to whom this information is entrusted will keep and use it for appropriate purposes. As stated by the Commissioner of Police, Katarina Carroll APM, during the hearing, the QPS "depends on having a high trust relationship with the public" and so "certainly issues around misusing information can erode that trust".[25] This has been acknowledged and acted upon by the then Police Commissioner, Ian Stewart, who issued directions to all staff in March 2016 and December 2018 on unlawful and inappropriate access to QPS information systems. The Commissioner warned staff that if they accessed information that was not connected to a purpose of one's duty, the conduct would be considered misconduct. Legislation provides that QPS officers and staff members are prohibited from disclosing information if that information has been obtained as a result of their employment with the QPS.[26]

The QPS undertakes a range of activities designed to promote ethical behaviour, discipline and professional practice to ensure members of the public have confidence in, and respect for, the police.[27] The total number of full-time equivalent staff in the QPS was 15,285 as at 30 June 2019 spread across five regions.

As shown in figure 1, although the QPS has recorded a decrease in the number of allegations regarding the misuse of confidential information in recent years, it still records a significant number of allegations, the highest by far amongst the seven agencies examined.

23 See also *QPS Annual Report 2018-2019*. Accessed from https://www.police.qld.gov.au/sites/default/files/2019-09/FINAL%20QPS%20AR%202018-19.pdf, p. 8

24 See *QPS Annual Report 2018-2019*. Accessed from https://www.police.qld.gov.au/sites/default/files/2019-09/FINAL%20QPS%20AR%202018-19.pdf

25 Evidence given by Katarina Carroll on 18 November 2019, p. 10

26 PSA Act, s. 10.1

27 See *QPS Annual Report 2018-2019*

Queensland Corrective Services

Queensland Corrective Services (QCS) is governed by the CS Act, which provides that the purpose of corrective services is community safety and crime prevention through the humane containment, supervision and rehabilitation of offenders.[28] The total number of full-time equivalent staff in QCS was 5054 as at June 2019.[29] The *QCS Annual Report 2018–19* states that 8773 prisoners are in custody and that its correctional facilities consist of 11 high-security prisons, 6 low-security prisons and 13 work camps. Fourteen prisons are outlined under Schedule 1 of the Corrective Services Regulation 2017.

In the course of their duties, corrective services officers frequently have to deal with confidential information. At times, this will involve collaboration with other Queensland government agencies. For example, corrective services officers are required to consider the individual risks and needs of prisoners and may make referrals to DoH staff regarding welfare, rehabilitation and community reintegration needs of prisoners, including at-risk management, medical needs and family welfare arrangements.[30] This information can include details regarding prisoner criminal history, family contacts, next of kin and health records. This presents a significant corruption risk for QCS, particularly from the potential for misuse of such confidential information.

The CCC's Taskforce Flaxton highlighted that the power of knowledge is intensified in custodial settings by the diverse legislated authority that correctional staff hold and the vulnerabilities of the prisoner population.[31] In this context, unauthorised access to and release of information can have severe consequences for the safety and security of prisoners as well as the overall correctional facility. For example, staff accessing and releasing information about a prisoner's offence, such as sex offences involving children, can directly affect the safety of that prisoner. Staff having access to confidential information also makes them a target for manipulation or coercion by prisoners or outside associates of prisoners. This has the potential to foster other corruption risks such as inappropriate relationships.[32]

The CS Act recognises that every member of society has certain basic human entitlements, and that, for this reason, an offender's entitlements, other than those that are necessarily diminished because of imprisonment or another court sentence, should be safeguarded.[33] Numerous safeguards are provided for explicitly within legislation and through QCS custodial operations practice directives. For example, under the Practice Directive "Daily Operations – Case Management", corrective services officers are required to promote the safety, security and good order of a corrective services facility through effective prisoner management.[34]

The QCS Practice Directive "Confidential Information – Disclosure of Confidential Information" provides that Inspectors and staff delegated by the Chief Executive to undertake investigations in relation to their role and functions have the power to inspect and copy any document kept at a corrective services facility that is relevant to the performance of their work.[35] However documents related to legal professional privilege are not permitted to be examined. As at the QPS, QCS staff are

28 CS Act, s. 3(1).

29 See *QCS Annual Report 2018-2019*. Accessed from https://www.publications.qld.gov.au/dataset/qcs-annual-reports/resource/ac3ac1b4-6161-4859-a2e8-87e800c49331, p.50

30 See Custodial Operations Practice Directive, Daily Operations – Case Management. Accessed from https://publications.qld.gov.au/dataset/qcs-procedures/resource/c39cafe1-5a7f-414d-9784-de111a668433

31 See http://www.ccc.qld.gov.au/corruption/taskforce-flaxton

32 CCC (2018). *Taskforce Flaxton: An examination of corruption risks and corruption in Queensland prisons*, p. 11-12. Accessed from https://www.ccc.qld.gov.au/publications/taskforce-flaxton

33 CS Act, s. 3(2)

34 See https://publications.qld.gov.au/dataset/qcs-procedures/resource/c39cafe1-5a7f-414d-9784-de111a668433

35 See https://publications.qld.gov.au/dataset/qcs-procedures/resource/69a90be3-d658-434c-bc46-e58c5e3553e3

prohibited from improperly disclosing confidential information. Section 341 of the CS Act outlines that an "informed person" must not disclose confidential information acquired by the informed person as a result of the performance of a function under the CS Act[36], without a permitted reason.[37]

Figure 1 shows that there has been a significant and sharp increase in the number of allegations regarding the misuse of confidential information within QCS. Although this increase may arguably have resulted from the recent prominence accorded to the intolerance of misuse of confidential information after Taskforce Flaxton, it still speaks of the weakness in QCS organisational systems and/or culture that prevents effective compliance with information privacy requirements.

Department of Education

The Department of Education (DoE) is responsible for the administration of the EGP Act. Section 5(1) outlines the objects of the Act including:

- to provide high-quality education to each child or young person in Queensland
- to provide universal access to high-quality State education
- to outline a range of education and training options for young people after they turn 16 years or complete year 10.

DoE consists of 73,741 staff, 94 per cent of whom are based in schools.[38]

In the performance of their functions under the EGP Act, DoE employees hold a special position of trust arising from the nature of their work. DoE employees exercise powers that have a significant impact on the lives of students and consequently there is a community expectation that these powers will be properly and prudently used.[39] DoE is required to access and store a significant amount of personal information about both employees and students. In the case of students, this can include, for example, information about their health and medical conditions, report cards and disciplinary documents.

The EGP Act requires that school staff members must give a written report of reasonable suspicions of suspected child abuse and neglect, regardless of whether the QPS is already aware of the matter.[40] All documents related to student protection concerns are to be stored in a "secure location" or OneSchool, an automated system in all Queensland state schools which provides teachers, administrators and principals with secure, easy access to information about students, curriculum, assessment and progress reporting, school facilities and school finance.[41] Unauthorised access to such information is a significant risk to both students and employees.

DoE provides various controls over its data, such as the Information Standards and Guidelines and Standard of Practice.[42] Also, the EGP Act requires that any person who has been a public service employee in the department, who in their capacity has gained or has access to personal information

---

36 CS Act, s. 341(2)

37 CS Act, s. 341(3)

38 See *DoE Annual Report 2018-2019*. Accessed from https://qed.qld.gov.au/det-publications/reports/Documents/annual-report/18-19/annual-report-2018-19.pdf, p. 56

39 See DoE Standard of Practice, February 2016. Accessed from https://qed.qldgov.au/workfordet/induction/det/inductionprogramsandresources/Documents/code-of-conduct-standard-of-practice.pdf

40 See DoE Procedure- Student Protection available at http://ppr.det.qld.gov.au/education/community/Procedure%20Attachments/Student%20Protection/student-protection.pdf

41 See *DoE Annual Report 2018-2019*, p. 98

42 See https://qed.qld.gov.au/workfordet/induction/det/inductionprogramsandresources/Documents/code-of-conduct-standard-of-practice.pdf

about a State school student, must not make a record of the information, use the information or disclose the information to anyone else.[43] This provision is supported by the DoE's policy on appropriate and ethical use of public resources, which ensures that "all officers are accountable for the departmental resources that they use, and that resource use is publicly defensible and clearly provides improved outcomes for the department's customers of the State as a whole".[44] Additionally, DoE implemented an Information Security policy in November 2018 that aims to protect information against unauthorised disclosure, access or use, loss or compromise, or a breach of privacy.[45]

Notwithstanding, DoE recorded a sharp increase in the number of allegations regarding misuse of confidential information in 2018–19, as shown in figure 1. This probably suggests that having policies in place, while important, may not be enough by itself to promote an effective organisational culture of compliance with information privacy requirements.

Department of Transport and Main Roads

DTMR discharges its statutory obligations under 23 Acts[46], including the *Transport Infrastructure Act 1994* and the *Transport Planning and Coordination Act 1994*. The overall object of both of these Acts is to provide a regime that allows for and encourages effective integrated planning and efficient management of a system of transport infrastructure.[47] Both Acts contain provisions regarding confidentiality. The *Transport Infrastructure Act 1994* provides a person must not, intentionally or recklessly, disclose, allow access to, record or use personal information.[48] The *Transport Planning and Coordination Act 1994* provides that a person must not disclose, record or use information gained through involvement in the administration of the Act, unless authorised under the Act.[49]

DTMR is comprised of 7102 full-time equivalent employees and 79 occupational groups spread across trade, professional, technical and administrative disciplines throughout Queensland.[50] DTMR plans, manages and delivers Queensland's integrated transport environment to achieve sustainable transport solutions for road, rail, and sea.

DTMR's legislative obligations are reflected in its Information Privacy Plan, as displayed on the department's website.[51] The plan provides a guideline for employees and contractors of the department who deal with personal information in relation to the functions and activities of the department. All employees, contractors and consultants within the department have responsibilities to ensure that the personal information they handle in their everyday duties is managed in accordance with the IP Act.

According to DTMR's Information Privacy Plan, DTMR is the largest holder of personal information in the Queensland public sector. The collection of personal information is a central part of many of DTMR's business activities. This information can include customer name, address, marital status, licence status and driving and fare evasion offence information. All datasets that hold personal information are reviewed from time to time by the Right to Information (RTI), Privacy and Complaints Management Team. The objective of these reviews is to ascertain across the department whether

---

43 EGPA, s. 426, other than for a reason set out in subsection 4.

44 See http://ppr.det.qld.gov.au/pif/policies/Documents/appropriate-and-ethical-use-of-public-resources.pdf, p. 1

45 See http://ppr.det.qld.gov.au/pif/policies/Documents/Information%20Security%20Policy.pdf

46 See *DTMR Annual Report 2018-2019*. Accessed from https://www.publications.qld.gov.au/dataset/annual-report-2018-2019-transport-and-main-roads/resource/e2e33266-db66-4afd-acae-bf741c4d179c, p. 4

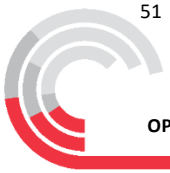
47 *Transport Infrastructure Act 1994*, s. 2(1)

48 *Transport Infrastructure Act 1994*, s. 105ZN

49 *Transport Planning and Coordination Act 1994*, s. 36GA

50 See *DTMR Annual Report 2018-2019*, p. 175

51 See https://www.tmr.qld.gov.au/Help/Privacy



records of personal information are being collected, stored, used and disclosed in accordance with the IPPs, and to assist in identifying measures that may be taken to reduce the risk brought about by non-compliance with the IPPs.

As shown in figure 1, DTMR recorded an increase in the number of allegations regarding misuse of confidential information in 2018–19.

Department of Health

The Department of Health (DoH), under the HHB Act, is responsible for the overall management of the Queensland public health system.[52] This responsibility is carried out by DoH in conjunction with 16 Hospital and Health Services (HHSs). The objective of the HHB Act is to establish a public sector health system that delivers high-quality hospital and other health services in Queensland, having regard to the principles and objectives of the national health system.[53] Among other strategies, the objective is achieved by strengthening local decision-making and accountability[54], and providing for State-wide health system management including health system planning, coordination and standard setting.[55]

Part 7 of the HHB Act stipulates specific confidentiality requirements for "designated persons" and "prescribed health practitioners".[56] That Part also sets out the duty of confidentiality and exceptions that permit the disclosure of confidential information by designated persons and prescribed health practitioners.

DoH employed 90,513 full-time equivalent (FTE) staff as at June 2019.[57] Of these, 12,293 FTE staff were employed by and worked in the department, including 4610 FTE staff in the Queensland Ambulance Service, 4343 FTE staff in Health Support Queensland, and 1458 FTE staff in eHealth Queensland.

HHSs are statutory bodies and are the principal providers of public sector health services.[58] The public sector health system is comprised of the HHSs and the department.[59] The overall management of the public sector health system is the responsibility of the department, through the chief executive (the system manager role).[60] Among others, the chief executive is responsible for monitoring the HHSs' performance and issuing binding health service directives to HHSs.[61] Safeguards are provided to protect the confidentiality of information that identifies persons who have received public sector health services.[62] When performing a function or exercising a power under the Act, the best interests of users of public sector health services should be the main consideration in all decisions and actions.[63]

---

52 See *DoH Annual Report 2018-2019*. Accessed from https://www.health.qld.gov.au/__data/assets/pdf_file/0019/882010/190927-DoH-Annual-Report-2018-19.pdf

53 HHB Act, s. 5(1)

54 HHB Act, s. 5(2)(a)

55 HHB Act, s. 5 (2)(b)

56 HHB Act, ss. 142 & 142A

57 See *DoH Annual Report 2018-2019*, p. 64

58 HHB Act, s.7(1)

59 HHB Act, s.8(1)

60 HHB Act, s.8(2)

61 HHB Act, s.8(3)

62 HHB ACT, s.12

63 HHB ACT, s. 13(1)(a)

When members of the public attend a health facility, a record is made that contains the person's name, address and contact details, nature of the problem, family history, diagnosis and treatment, test results, and Medicare and other Commonwealth benefit card details.[64] Updated information is added to each person's record upon attendance. Failure to properly safeguard this information poses a risk to both the safety and privacy of the person.

Confidentiality requirements are further supported by the DoH Use of Information and Communications Technology (ICT) Services Standard QH-IMP-032:2016 (the Standard). Clause 3.2.4 places an obligation on "all authorised users" to ensure they only access information that is reasonably required for and consistent with the performance of their role and as approved by their line manager or supervisor.[65] The Standard outlines situations that would constitute unauthorised use, such as accessing information not directly related to an authorised user's duties, and searching health information on behalf of an acquaintance or merely out of curiosity.

The DoH's Privacy Plan sets out details of the types of personal information held, and how the information is dealt with in accordance with both the IP Act and the HHB Act.[66] This plan refers to DoH and the HHSs collectively as Queensland Health. The plan defines personal information as any information or opinion about an identifiable living individual.

From the above, DoH seems to have quite a robust system in place for building the needed information privacy culture. However, like DTMR, DoH recorded an increase in the number of allegations relating to misuse of confidential information in 2018–19, as shown in figure 1. Although DoH's figure that year was lower than that of other subject agencies, the increase of allegations recorded in that year is an issue of concern.

Gold Coast Hospital and Health Service

Gold Coast Hospital and Health Service (GCHHS) was established under the HHB Act on 1 July 2012.[67] GCHHS's main function is to deliver the hospital services, teaching, research and other services stated in the service agreement for the Service.[68] GCHHS has a workforce consisting of 8262 full-time equivalent (FTE) staff.[69] GCHHS delivers a broad range of secondary and tertiary health services from three hospitals, 13 community located facilities, and two major Allied Health Precincts at Southport and Robina.[70]

As with DoH, GCHHS is bound by Part 7 of the HHB Act. This is specified in the GCHHS Privacy Plan, which states that "Gold Coast Health takes the necessary steps to protect personal information against loss, unauthorised access, use, modification or disclosure, and against other misuse".[71] These necessary steps include password protection for accessing the GCHHS' electronic systems. Further, it is noted in the GCHHS's Privacy Plan that security classifications are applied to all sensitive documents to ensure that classified sensitive documents are protected from unauthorised access.

---

64 See https://www.health.qld.gov.au/system-governance/records-privacy/health-personal

65 See https://www.health.qld.gov.au/__data/assets/pdf_file/0030/397308/qh-imp-032-1.pdf

66 See https://www.health.qld.gov.au/global/privacy

67 See *Gold Coast HHS Annual Report 2018-2019*. Accessed from https://www.goldcoast.health.qld.gov.au/about-us/publications/annual-report

68 HHB Act s. 19(1)

69 See *Gold Coast HHS Annual Report 2018-2019*, p. 36

70 See *Gold Coast HHS Annual Report 2018-2019*

71 See https://www.publications.qld.gov.au/dataset/gold-coast-hospital-and-health-service-plans/resource/3fb7332e-edc2-47bc-affa-0a9503286c1f, p. 6

Like many agencies, GCHHS experienced an increase in the number of allegations relating to misuse of confidential information in 2018–19, as shown in figure 1.

Mackay Hospital and Health Service

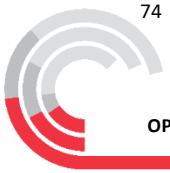
Mackay Hospital and Health Service (Mackay HHS) was established on 1 July 2012, and its responsibilities are set out in the HHB Act.[72] Mackay HHS operates according to the service agreement with DoH, which outlines the services to be provided, funding arrangements, and performance indicators and targets. Mackay HHS is responsible for the delivery of public hospital and health services to an estimated resident population of 182,000. Mackay HHS has the full-time equivalent (FTE) staff population of 2388.[73] Like DoH and GCHHS, Mackay HHS is bound by Part 7 of the HHB Act. Mackay HHS has in place strict confidentiality requirements in the management of information. It is emphasised in the document entitled *Your Health Record and Personal Information* that it is an offence for staff to give information about patients to anyone, except as permitted by legislation.[74]

Like DoH and GCHHS, Mackay HHS also recorded an increase in the number of allegations regarding misuse of confidential information in 2018–19, as shown in figure 1.

72 See *Mackay HHS Annual Report 2018-2019*. Accessed from http://www.mackay.health.qld.gov.au/about-us/publications/

73 See *Mackay HHS Annual Report 2018-2019*, p. 21

74 See http://www.mackay.health.qld.gov.au/patients-and-visitors/access-your-medical-records/



Part 2 – Misuse of information – causes and consequences

Chapter 4 looks at the impact of breaches on both the people whose information has been accessed and the agency.

Chapter 5 looks at the reasons why, despite agency safeguards and warnings, employees continue to inappropriately access the information they have been entrusted to protect.

Chapter 4 — Impact assessment

Analysis of the evidence gathered throughout the course of Operation Impala has shown that the consequences for misusing confidential information can be significant for both public sector agencies and individual members of the public. Failure to protect confidential information "exposes individuals to risk, erodes trust and confidence in government, jeopardises public take-up of services, and damages agency reputation".[75]

Risks identified

Executive leaders and delegates of the seven subject public sector agencies were called to give evidence during Operation Impala's public hearing. Witnesses were each asked what they considered to be the greatest risks to managing privacy within their respective agencies. Three common risks were identified:

- Managing the obligations of storing large volumes of information that are diverse in nature, and involve different types of associated risks
- Ensuring consistency in approaches to information security and privacy protection where there are smaller, decentralised entities that may be geographically widespread, and
- Being informed of and responding efficiently to advances in technologies that might impact on approaches to information security, access control systems and/or database usability.

The OIC in its submission to Operation Impala outlined that information collected by public sector agencies may comprise: [76]

> *…health and education information, details about contact with the criminal justice system, addresses, dates of birth and phone numbers, driver licence information, and biometric information…Data may also be collected that could track individuals' movements and daily activities, such as transport usage.*

Striking a balance between operational needs and information security was identified as being a difficult exercise. Tony Cook APM, Director-General of DoE, told the CCC in evidence that striking the balance between "security provisions" and the "useability of that database" is one of the department's "greatest challenges".[77]

Ongoing advances in the ICT space are expected to continue to generate new ways to access and misuse confidential information stored on databases, which was not previously available or contemplated when using paper-based records[78]. That said, advances in ICT assist the creation and maturity of better systems to safeguard against, monitor and detect incidents of unauthorised use. One such ICT advance is the advent of QPS QLiTE Devices. These hand-held mobility tools enable police to conduct QPRIME searches, move-on directions and other policing activities on the spot.[79] A further example is DoH's Bring Your Own Devices (BYOD) initiative that allows authorised users access to ICT systems containing Queensland Health information via their own personal devices at remote locations.[80]

---

75 Submission given by OIC on 9 October 2019 (Submission 2), p. 4.

76 Submission given by OIC on 9 October 2019 (Submission 2), p.4.

77 Evidence given by Tony Cook on 12 November 2019, p. 10.

78 Evidence given by Hannah Bloch on 13 November 2019, p. 13.

79 Exhibit 135 - Statement from Timothy Dillon - PSBA (redacted), p. 8.

80 "BYOD Self-managed service", Queensland Health, Department of Health Standard QH-IMP-032-3:2017, p. 1.

Whilst this technology improves public sector agency capabilities by providing a more efficient approach to service delivery, it also increases the risk of staff accessing information for a purpose unrelated to their official work duties.[81] This conduct may go undetected unless appropriate and adaptable systems and procedures are put in place. A key challenge for government is striking a balance between ensuring authorised personnel have timely access to the confidential information necessary to perform their job and appropriately managing the range of information that public sector agencies hold, in order to meet the expectations of Queenslanders.[82]

Organisational impact

Members of the public should be able to trust that public sector agencies will deal with their confidential information appropriately and according to legislative and policy requirements. Failure to do so may negatively impact the reputation of an agency and/or result in increased litigation.

Misuse of confidential information is likely to erode public trust and adversely impact on organisational reputation. QCS described this as an "unacceptable reputational risk"[83] in its public submission to the CCC, noting that instances of misuse of confidential information risk impeding the agency's ability to perform its functions by "undermining community confidence in the criminal justice system".[84]

Misuse of confidential information exposes agencies to a heightened risk of litigation. The case of ZIL v Queensland Police Service[85] highlights the reality of this risk. It is a significant case not only for the QPS, but for all public sector agencies. For this reason, a summary of the matter is given below and will be referred to throughout the report.

Case study: Disclosure of information by QPS officer Neil Punchard (ZIL v Queensland Police Service)

Between 30 July 2013 and 19 May 2016, Senior Constable (SC) Neil Punchard accessed the QPS database QPRIME on nine occasions. SC Punchard accessed QPRIME to ascertain the concerned party's (CP's) then residential address and disclosed this to the CP's ex-husband, a childhood friend of Punchard's. SC Punchard's access was discovered due to the chance discovery of text messages between him and the ex-husband.

Referral to CCC

On 23 June 2016, the CP made a complaint to the CCC about SC Punchard. She provided a document purporting to record messages between SC Punchard and her ex-husband. The complaint was referred by the CCC to the QPS to investigate, subject to CCC oversight.

CCC oversight of QPS investigation

On 7 April 2017, the QPS found there was insufficient evidence to support criminal charges. However, sufficient evidence existed to substantiate police misconduct against SC Punchard. A sanction of one (1) pay-point reduction (from 2.10 to 2.9) for a period of 12 months was imposed as a result of subsequent internal disciplinary proceedings. The CCC elected not to review the decision.

81 Evidence given by Rod Francisco on 12 November 2019, p. 6.

82 Evidence given by Andrew Mills on 20 November 2019, p. 3-4.

83 Submission given by QCS on 10 October 2019 (Submission 1), p. 11

84 Submission given by QCS on 10 October 2019 (Submission 1), p. 11

85 [2019] QCAT 79.

The CP met with the Commissioner of Police on 9 May 2018 and expressed concern regarding the objectivity of the investigation and the welfare of her family, due to SC Punchard's association with her ex-husband. The Commissioner subsequently ordered that the QPS internal investigation be reviewed by a senior officer, subject to a senior member of the CCC providing oversight of the review.

On 13 August 2018, the QPS determined that the matter was appropriately investigated, the outcome was consistent with comparable matters at the time, and the evidence available did not support criminal proceedings being instituted. This review was sent to the CCC on 21 August 2018.

The CCC conducted an overview of the QPS' review which was finalised on 25 September 2018. The CCC asserted a criminal prosecution should have been commenced. Evidence from the QPS' own records could have been obtained to prove, by admissible evidence to the relevant standard, that SC Punchard accessed and disclosed information stored on QPRIME without authorisation. The CCC recommended that efforts should be made to assemble relevant evidence to facilitate the charging of SC Punchard with offences of computer hacking as soon as practicable. SC Punchard was subsequently charged with nine counts of computer hacking and misuse on 14 December 2018 and issued with a Notice to Appear before the Brisbane Magistrates Court on 20 January 2019.

Criminal prosecution

On 11 September 2019, SC Punchard pleaded guilty to nine counts of computer hacking and misuse pursuant to s. 408E (1) and (2) of the Criminal Code and was sentenced on 14 October 2019 to two months imprisonment, wholly suspended for 18 months for each offence (concurrent). Two of the charges related to SC Punchard disclosing the CP's ex-partner's unit number.

In sentencing, Magistrate Previtera asserted that, "what is serious about the offending is that you knew that what you were doing was wrong". Magistrate Previtera highlighted that police officers are duty bound "to uphold the law and the public must be entitled to rely upon their integrity".[86] Punchard's offending was a significant risk in relation to the safety of a member of the public. Members of the public rightly expect that police "will protect them and certainly not take any action to place them at any degree of risk".[87] This sentence is currently subject to an appeal.

QCAT litigation

The CP made a privacy complaint to the Information Commissioner about the incident. Due to unsuccessful mediation attempts, the Information Commissioner referred the complaint to QCAT on 30 April 2018.[88] On 9 November 2018, the CP submitted to QCAT that, among other things, the QPS breached IPP4 of the IP Act by failing to take reasonable steps to prevent unauthorised use or disclosure of her personal information, namely her residential address, by SC Punchard. On 27 March 2019, QCAT found that the QPS had breached IPP4. Member Gardiner stated that there was no evidence the QPS employed any "systemic auditing procedures" of access to QPRIME.[89] This lack of an auditing system could have jeopardised the safety of the CP and her family because of the based on the information accessed and disclosed. Further, there was a lack of any specific consideration by the QPS of the CP being a vulnerable person, namely a domestic violence victim. The tribunal found that "the QPS allowed use of this information for a purpose other than the purpose for which it was obtained".[90]

On 6 December 2019, the tribunal ordered dismissal of the QPS' application for an extension of time to appeal, refused the original application for the appeal and remitted the issue of compensation to the tribunal of first instance.[91]

86 *Police and Neil Glen Punchard*, Decision in Brisbane Magistrates Court on 14 October 2019 5.

87 *Police and Neil Glen Punchard*, Decision in Brisbane Magistrates Court on 14 October 2019 6.

88 ZIL v Punchard & Anor [2018] QCAT 274 [5].

89 ZIL v Queensland Police Service [2019] QCAT 79

90 [2019] QCAT 79 [57]

91 Queensland Police Service v ZIL [2019] QCATA [26 – 29].

The QPS' handling of this matter has been significantly and publicly criticised. Police Minister Mark Ryan added to the debate, broadcasting his view to the media that the QPS should quickly resolve the matter to prevent compounding the victim's trauma.[92] This case demonstrates the impact that misuse of confidential information can have on the individuals whose information is accessed and on an organisation's reputation, and shows how an agency can put itself at risk of litigation.

Impact on victims of misuse of confidential information

Evidence obtained during the course of Operation Impala highlighted the far-reaching and long-term impact of misuse of confidential information on victims.

Circumstances affecting the level of risk

Misuse of confidential information is not a victimless crime and it can happen to anyone who engages with a public sector agency, although the individual circumstances and the associated level of risk may vary.

- Executive Director of People at Mackay HHS, Rod Francisco, who specialises in human resources management, business management and industrial relations, gave evidence about "high-profile patients"[93] who had been involved in a shark attack at the Whitsunday Islands and attracted significant media attention. A confidentiality alert was placed on the files of the two patients involved within an hour of file creation. It was considered that the two patients were at risk of persons misusing their information, including the potential for HHS staff to view their patient files out of curiosity.
- Celebrity Magda Szubanski voiced concerns after an experience with nursing staff while in post-operative hospital care. The nurse had tweeted about looking after Ms Szubanski in hospital, thereby sharing confidential information about a patient on social media. Responding to the tweet, Ms Szubanski said it had shaken her up: "The thought that I'm not safe at my most vulnerable". Ms Szubanski tweeted that the event had been "upsetting", leaving her feeling "very vulnerable and unsafe".[94]
- A case in New Zealand shows how misuse of confidential information can have ongoing and substantial ramifications. A former health employee (the complainant) had her patient file accessed multiple times by a colleague (the subject officer) without there being a work-related purpose for doing so. It became apparent the subject officer knew about the complainant's sensitive health information. Following an audit by management of access to the complainant's patient file (carried out at the request of the complainant), it was revealed that other members of staff had also accessed the complainant's file. The complainant suffered from nightmares, high levels of anxiety, was fearful of staff continuing to browse her health information, and ultimately lost complete trust in the agency.[95]

92 B. Smee, "Minister urges Queensland police to resolve domestic violence victim's compensation case", *The Guardian*, 30 October 2019 https://www.theguardian.com/australia-news/2019/oct/30/minister-urges-queensland-police-to-resolve-domestic-violence-victims-compensation-case.

93 Evidence given by Rod Francisco on 12 November 2019, p.20

94 M. Friedlander, " 'I feel very vulnerable and unsafe': Magda Szubanski is left 'shaken' after a nurse tweeted about the actress' recent hospital stay in a major privacy breach", *Daily Mail*, 2 December 2019, https://www.msn.com/en-au/news/australia/i-feel-very-vulnerable-and-unsafe-magda-szubanski-is-left-shaken-after-a-nurse-tweeted-about-the-actress-recent-hospital-stay-in-a-major-privacy-breach/ar-BBXFdKJ?ocid=ientp

95 https://www.privacy.org.nz/news-and-publications/case-notes-and-court-decisions/case-note-269784-2016-nz-privcmr-3-employee-repeatedly-accessed-health-records-without-proper-reason/

- An ABC news report that aired on 17 December 2019 highlighted that anyone, even former Australian Federal Police (AFP) commissioners, can be victims of privacy breaches.[96]

Agency identification of categories of people (including vulnerable and high-profile persons) whose personal information requires additional confidentiality safeguards is discussed in chapter 9.

Impacts experienced by domestic and family violence victims

The CEO of the Domestic Violence Prevention Centre, Rosemary O'Malley, gave evidence about her experience of the impact that misuse of a person's confidential information can have in situations involving domestic and family violence.

Ms O'Malley identified a range of potential impacts including, but not limited to:[97]

- psychological and emotional harm
- reduced likelihood of engagement with necessary support agencies, law enforcement and/or prosecutorial agencies in the future
- negative impacts on the victim's ability to parent
- costs associated with moving house, such as removalist fees and bonds required to lease a different property, in the event of contact details being disclosed to a respondent
- children having to change schools, disrupting their connection to friends, support networks and education, and
- change of employment, in turn forgoing accrued leave, with potential impacts on their career trajectory.

Impacts on community perceptions of public sector agencies

Renee Eaves, a social justice advocate, who had been adversely affected by having had her confidential information misused, provided evidence about the impact that such misuse can have on the community's perception of public sector agencies. She stated: [98]

> *…at the heart of misuse are real people, real people whose lives are affected, and there has been little focus yet on the ripple effect of that misuse.*
>
> *…It goes against what we learn as children, that they're [the QPS] the people we can trust, the ones that we can turn to that have the highest integrity.*

Personal impacts and flow-on effects

When Ms Eaves was asked about the personal impacts she experienced as a result of her privacy being breached, she told the CCC that she:[99]

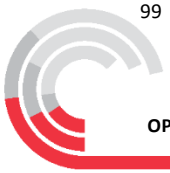
> *…felt extremely helpless—stressed, frustrated, triggered. And, as a result, the only option I had at that time was to pack my things… and move cities. So the impact on my privacy being breached simply cannot be understated.*

96 Paul Farrell, "Medicare card details being sold on the dark web", 7.30, ABC News, 17 December 2019, https://www.abc.net.au/7.30/medicare-card-details-being-sold-on-the-dark-web/11808150.

97 Evidence given by Rosemary O'Malley on 19 November 2019, p. 5-6.

98 Evidence given by Renee Eaves on 19 November 2019, p. 4.

99 Evidence given by Renee Eaves on 19 November 2019, p. 8.



Ms Eaves is a social justice advocate who has worked with a number of people who had experienced breaches of their privacy. Ms Eaves was asked about the emotional, psychological, financial and other personal impacts that flow from misuse of someone's confidential information. Referring to circumstances involving relocating with children, Ms Eaves stated:

> *The cost to your mental, financial, physical, spiritual, your social support, it's enormous. It is wide-reaching. And like I say it can't be understated.*[100]

Ms Eaves' evidence was reiterated by a witness[101] whose privacy was breached when QPS officer Neil Punchard unlawfully accessed her QPRIME file and disclosed her personal residential details to his school friend, her ex-partner.[102] The witness was going through an acrimonious separation from her ex-partner, and she was not disclosing her address details to him at that time.

When asked about how this personally affected her, the witness said the unauthorised access and disclosure effectively imposed "a life sentence"[103] on her and her children. She said these consequences were far greater than the privacy breach itself. The witness relocated on two occasions during the course of the separation and the privacy breach.[104] The witness told the CCC this brought about feelings of guilt, as her family were happy with their existing living arrangements, which generated feelings of instability, hypervigilance and uncertainty.[105] The witness said she also sought medical assistance to address heart palpitations and insomnia that she said stemmed from the privacy breach and how it was dealt with thereafter.[106] In addition, her children have required extensive counselling, which remains ongoing years later.[107]

The Privacy Commissioner told the CCC with reference to his experience in the OIC's complaints jurisdiction:

> *I've certainly heard the voice of anguish in complaints. And, yes, it's seriously impactful on some individuals and particularly difficult to recover from in some instances.*
>
> *…the impacts on the specific individual in a specific case cannot be underestimated and psychological harm and…mental anguish …they're hard to put a price on.*
>
> *So once something's known it can't become unknown…You know that there's some that's just irreversible. Death I suppose is the worst sort of physical outcome that's irreversible. But…the whole gamut of damage can occur.*
>
> *…there's this high suicide rate in this country and I think any impact on mental health through these breaches could contribute to that too.*

This evidence illustrates the range of consequences that can arise and impact on individuals and organisations from the misuse of a person's confidential information. It is therefore imperative that agencies take steps to avoid and mitigate the incidence of information misuse.

---

100 Evidence given by Renee Eaves on 19 November 2019, p. 10.

101 The identity of this witness is confidential, at her request.

102 See case study on pages 42–43

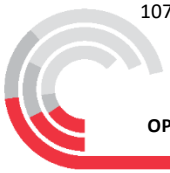
103 Evidence given by an anonymous witness on 25 November 2019, p. 5.

104 Evidence given by an anonymous witness on 25 November 2019, p. 5.

105 Evidence given by an anonymous witness on 25 November 2019, p. 5.

106 Evidence given by an anonymous witness on 25 November 2019, p. 7

107 Evidence given by an anonymous witness on 25 November 2019, p. 20.



Chapter 5 – Drivers

This chapter of the report examines why employees access and misuse confidential information — that is, what motives drive such behaviour? Once identified, these motivations should also be considered as potential corruption risk factors by agencies.

Motivations (and related risks) relating to the misuse of confidential information, like the evaluation of any risk, require an evaluation of the probability that the misuse will happen and the consequences of the misuse.[108] Internal risks as a result of employee misconduct are a significant challenge that agencies face in safeguarding their information assets. In an insight report by the Office of the Australian Information Commissioner (OAIC), it was evident that the insider "human factor" accounted for 35 per cent of data breaches over a one-year period (April 2018 to March 2019).[109] Internal access to confidential information is therefore recognised as a major contributor to misuse of that information. This challenge increases as public sector agencies shift to the use of ICT as the most efficient system for management of their information assets.[110] In a recent survey of the Victorian Police, for instance, 87 per cent of employees agreed that there was an opportunity for misuse of information to occur.[111]

The potential negative impact that employees can have on a public sector agency's reputation was acknowledged by witnesses during the hearing. For instance, the Commissioner of Police, Katarina Carroll, noted that the greatest concern to the QPS was the improper behaviour of some officers undermining the legitimacy of the QPS's role and the confidence that the public had in the QPS as a trustworthy institution to make sure that information that comes to the QPS is used appropriately and for the right reasons.[112] Similarly, Hannah Bloch, Executive Director, People and Corporate Services, GCHHS, emphasised that one of the single greatest risks to that entity was the significant adoption of ICT in the management of their information assets, as this made it easy for staff to be able to access information in different ways.[113]

Public officers who improperly access confidential information from public sector databases can be motivated by a number of things. In serious instances, information may be accessed with an intention to pass the information on to others, or to profit from it, to intimidate others, or frustrate investigations or proper legal processes. Sometimes, curiosity is the sole motivation, but even this access represents a serious incidence of misuse.[114]

---

108 Evidence given by Dr Russell Smith on 11 November 2019, p. 10

109 OAIC (2019). *Notifiable Data Breaches Scheme 12-month Insights Report*, p. 13. Accessed from https://www.oaic.gov.au/assets/privacy/notifiable-data-breaches-scheme/statistics/ndb-scheme-12month-insights-report.pdf

110 Hutchings, A., & Jorna, P. (2015). *Misuse of information and communications technology within the public sector*, p. 1. Accessed from https://aic.gov.au/publications/tandi/tandi470

111 IBAC (2017). *Perceptions of corruption: Survey of Victorian Police employees*, p. 7. Accessed from https://www.ibac.vic.gov.au/docs/default-source/research-documents/perceptions-of-corruption-victoria-police.pdf?sfvrsn=482f7075_7

112 Evidence given by Katarina Carroll on 18 November 2019, p. 7

113 Evidence given by Hannah Bloch on 13 November 2019, p. 5

114 CCC (2019). *Improper access to public sector databases, no. 2*, p. 3. Accessed from https://www.ccc.qld.gov.au/sites/default/files/Docs/Publications/CCC/Prevention-in-Focus-Improper-access-to-public-sector-databases-no2-2019.pdf

Accordingly, it is important to understand why employees misuse confidential information. This chapter explores these motivations in detail, supported by case studies, to set the context for recommendations for reform in later chapters. (It should be noted that the following motivations are not mutually exclusive and an employee's conduct could be categorised under one or more of the following classifications.)

Personal interest

Personal interest, in the form of curiosity,[115] is one driver for public sector employees to misuse confidential information. Examples may include employees viewing records associated with themselves, neighbours, friends, celebrities, politicians, current or former partners, family members or relatives, as well as people involved in incidents that have received significant media coverage. The danger with this type of access is that it is quite difficult to detect as, in most of these cases, the people whose information has been accessed do not become aware of the breach. When they do, it has the potential to erode public trust in the agency (as described in Chapter 4).

During the hearing, witnesses from the subject agencies agreed that their employees' curiosity was by far the most common motivator for accessing confidential information. For instance Ms Bloch stated that:

> *…the new report that we've provided, the P2Sentinel report, we're able to identify staff accessing their own record or a family member's record and that has resulted in an increase in cases being referred to the Crime and Corruption Commission.*[116]

Further, QCS Commissioner Dr Peter Martin stated that some of his officers would access confidential information out of voyeurism, with no good and legitimate reason – they were merely curious about what information was held in the system.[117] QCS further emphasised in its submission that "the majority of incidents involving improper access of confidential information may occur through curiosity and misadventure".[118] Employees' ability to satisfy their curiosity has increased with the shift from paper-based records to the use of ICT systems. This issue was recognised by Dr John Wakefield, Director-General of DoH, during the hearing:

> *… I think the commonest intentional breach that certainly I have observed is an individual person, clinician, looking at their own clinical records; whereas previously they'd have to go to the records department and get their own records out. And whilst that may not be malicious … I think from a cultural perspective we've still got work to do to remind people that that's something that's not appropriate.*[119]

The issue of personal interest (curiosity) also appeared to be linked to officers who became bored at work and were looking for a way to pass the time. The issue of boredom was particularly highlighted by the QCS Commissioner as a key motivating factor for some QCS employees:

> *We've got also a workforce where some of our people have significant time on their hands where issues and elements of boredom might very well come into play and these factors combine to ultimately create a difficult and a challenging circumstances for us.*[120]

---

115 IPPA WA (2016). Information integrity pathway / roadmap for reform, p. 5. Accessed from http://www.wa.ipaa.org.au/content/docs/2016/Research-Day/Papers/S3.1_Do_government_organisations.pdf

116 Evidence given by Hannah Bloch on 13 November 2019, p. 8

117 Evidence given by Dr Peter Martin on 11 November 2019, p. 21

118 Submission given by QCS on 10 October 2019 (Submission 1), p. 6

119 Evidence given by Dr John Wakefield on 14 November 2019, p. 10

120 Evidence given by Dr Peter Martin on 11 November 2019, p. 21

Other examples of this type of access were also given.

- In May 2017, a QPS officer was fined $4000 after pleading guilty to one count of computer hacking. It became evident that the officer accessed records from the QPRIME database in relation to members of his family, other police officers and the former partner of his wife. There was no evidence that the information was passed on to a third party.[121]
- During the hearing, a case study regarding a QCS officer was discussed. The officer had, without authority and for their own personal interest, accessed the personal information of a person met on an online platform.[122] As the officer was no longer an employee of QCS at the time of decision making, a post-separation disciplinary declaration was made.[123]

The issue of access motivated by curiosity, especially in relation to the QPS, has been considered, by some, to be a grey area regarding the circumstances in which this becomes inappropriate or unlawful. During the hearing Ian Leavers of the QPUE explained it was because the police, in order to provide the safety needed by the public, were generally trained to be curious.[124] In a recent article, Mick Barnes, the QPUE Secretary, stated that because the good intentions of QPS officers could lead to accusations of hacking, officers were more likely to disengage, which left the "community to suffer because of lack of appropriate policing".[125] However, the Commissioner of Police, Katarina Carroll, clarified that, in as much as police officers needed to be curious in order to provide the safety needed by the people of Queensland, it was expected that their curiosity should always be in line with official duties.[126]

Case study: Employee accessed details of a complaint against them (DoE)

A DoE employee was alleged to have inappropriately accessed a departmental database to view details of a complaint relating to her personal conduct. It is further alleged the employee again inappropriately accessed records pertaining to the complaints against her, despite having been advised not to as part of her ongoing discipline process.

An audit of the computer records indicated the employee first accessed documents relating to the complaint approximately four days after the complaint was made. The audit further identified the employee subsequently accessed the documents a number of times throughout the day. During the investigation the employee claimed she accidently found the documents when she was looking for another file she had created and saved. Risk management action was taken to remove "people's access to complaint records".

Later, during the department's management of this matter, additional concerns were raised, alleging the employee engaged in further inappropriate conduct whereby she again accessed records pertaining to the complaints against her, despite having been advised not to as part of her ongoing discipline process.

The department referred the matter to the QPS for consideration. The matter has been referred to Integrity and Employee Relations for monitoring of any QPS involvement and subsequent consideration of a department investigation.

---

121 CCC (2019). *Improper access to public sector databases: what you should know*, p. 2. Accessed from https://www.ccc.qld.gov.au/sites/default/files/Docs/Publications/CCC/Prevention-in-Focus-Improper-access-to-public-sector-databases-2018.pdf

122 Evidence given by Kim Papalia on 15 November 2019, p. 6-7

123 Evidence given by Kim Papalia on 15 November 2019, p. 6-7; see also Exhibit 85 of the public hearing

124 Evidence given by Ian Leavers on 18 November 2019, p. 10

125 Lynch, C. (2019). "Cop charged with hacking police system in south-east Queensland", *Brisbane Times*, 16 July 2019. Access from https://www.brisbanetimes.com.au/national/queensland/cop-charged-with-hacking-police-system-in-south-east-queensland-20190716-p527t7.html

126 Evidence given by Katarina Carroll on 18 November 2019, p. 15

Material benefit

Another factor that influences public officers to improperly access confidential information is the desire to gain material benefit. The benefit gained could be of a personal or commercial nature. In certain circumstances, employees of public sector agencies may be targeted to provide confidential information for financial or other benefits.[127] It is evident that public servants are "particularly at risk of being invited to act corruptly because of their access to confidential personal information".[128]

The CCC is of the view that two agencies whose employees are most likely to be targeted by organised crime groups, and sometimes private investigators, to provide confidential information and/or issue fraudulent documents are the QPS and DTMR. The police, for instance, can be targeted due to their general access to law enforcement systems.[129] In 2016 *The Age* highlighted that Victoria Police documents containing information from a secret law-enforcement database were found in a nightclub while the police were there undertaking drug-related searches.[130] The report also alleged the secret information was passed on by a detective to a former police officer linked to the nightclub.

During the hearing Dr Russell Smith stated that:

> *I think the main problem in terms of the organised crime infiltration aspect is that police hold a great deal of sensitive information about ongoing investigations… and if that information is made available to criminals, particularly those in organised crime groups, then that's particularly valuable in enabling them to tailor their activities to avoid detection… And also to obtain information about people within government departments who could be easily corrupted.*[131]

Further, where there is information that might be valuable to organised crime groups or members of the public (for example, driver licence information), public officers are more likely to be targeted and are mostly influenced with financial benefits to misuse and/or falsify information.[132]

Case study: Fraudulent issue of licences: Operation Danish (DTMR)

On 15 December 2012, the then boyfriend of DTMR employee Sheree Tritton contacted police and reported that his now ex-girlfriend was accessing DTMR records and providing addresses and other information to third parties.

Following a joint investigation between the CCC, the QPS and DTMR, Tritton was charged by the CCC with 94 criminal offences, including 88 separate counts of official corruption. The court found Tritton fraudulently issued or transferred 31 vehicle registrations and issued or upgraded 57 driver licences between 1 July 2012 and 13 December 2013, and received at least $20,000 in cash for the fraudulent transactions. Tritton was sentenced to four years imprisonment to serve six months, after which the sentence was suspended for four years, for fraudulently issuing driver licences, licence upgrades and vehicle registrations in return for cash payments.

---

127 IBAC. (2019). *Unauthorised access and disclosure of information held by Victoria Police*, p. 19. Accessed from https://www.ibac.vic.gov.au/publications-and-resources/article/unauthorised-access-and-disclosure-of-information-held-by-victoria-police

128 Smith, R., Oberman, T., & Fuller, G. (2018). *Understanding and responding to serious and organised crime involvement in public sector corruption*, p. 1. Accessed from https://aic.gov.au/publications/tandi/tandi534

129 IBAC. (2019). *Unauthorised access and disclosure of information held by Victoria Police*, p. 19

130 Mckenzie, N., Baker, R., Silvester, J., & Houston, C. (2016). "Nightclubs, dirty cops, drugs and leaks: the inside story", *The Age*, 23 September 2016. Accessed from https://www.theage.com.au/national/victoria/nightclubs-dirty-cops-drugs-and-leaks-the-inside-story-20160923-grncbj.html

131 Evidence given by Dr Russell Smith on 11 November 2019, p. 12

132 Evidence given by Dr Russell Smith on 11 November 2019, p. 12

Case study: Police officers supplied information to private investigator (QPS)

During a CCC investigation it was identified that two Detective Senior Constables (a married couple) were providing information to a licensed private investigator, who was the female officer's brother-in-law. An audit of QPRIME activity records for both officers found that they had conducted numerous checks unrelated to their duties. CCC investigations established that the officers were supplying information to the female officer's brother-in-law to assist him in his private investigation business. Specifically, the investigator specialised in surveillance, and was regularly obtaining information regarding his targets from the officers.

The two officers and the private investigator were charged with offences of computer hacking and misuse under s. 408E of the Criminal Code. The female officer pleaded guilty to 14 charges of computer hacking and was placed on probation for 30 months; no conviction was recorded. The male officer pleaded guilty to seven counts of computer hacking. He was initially sentenced to six months imprisonment, to be suspended for 15 months. This decision was overturned on appeal and replaced with a $2000 fine; no conviction was recorded. The private investigator entered a plea of guilty on 21 charges of computer hacking and was placed on probation for 18 months and ordered to perform 240 hours of community service; no conviction was recorded.

The Magistrate did not consider the matter to be less serious due to there being no financial benefit. For the private investigator, benefit was obtained by getting quick jobs which led to financial gain. For the police officers, although no direct benefit was identified, the benefit was in assisting a family member.

Relationships

Relationships are another factor that can cause public sector employees to inappropriately access and/or release confidential information to third parties.[133] These relationships may involve organised crime groups or other people, such as private investigators, calling on favours or using threats to request access to confidential information. For example, in 2017, a former police officer who had become a private investigator was under investigation for seeking official police information from a former colleague. Both had worked as detectives with the Victorian Police.[134] Both the private investigator and the police officer who had engaged in the unauthorised access to and disclosure of confidential information pleaded guilty to seven counts of misconduct in public office for illegally accessing the police database between 2011 and 2017. In September 2019, the judge stated that the relationship between the police officer and the private investigator was corrupt, jailed the police officer for six months and also ordered him to perform 100 hours of community work.[135] Although the private investigator was spared a jail term due to his mental health issues, he was ordered to complete 200 hours of unpaid community work.[136]

Family relationships, friendships or other networks may also induce public sector officers to inappropriately access confidential information. In these cases, two types of breaches are most likely to occur: the first is unauthorised access to confidential information about a relative or friend; and the second is unauthorised disclosure of that information.

133 CCC (2019). *Improper access to public sector databases, no. 2*, p. 2. Accessed from https://www.ccc.qld.gov.au/sites/default/files/Docs/Publications/CCC/Prevention-in-Focus-Improper-access-to-public-sector-databases-no2-2019.pdf

134 IBAC (2019). *Unauthorised access and disclosure of information held by Victoria Police*, p. 21.

135 More, Georgie (2019). "Ex-policeman jailed for passing data to private eye", *The Age*, 18 September 2019. Accessed from https://www.theage.com.au/national/victoria/ex-policeman-jailed-for-passing-data-to-private-eye-20190918-p52ski.html

136 More, Georgie (2019). "Ex-policeman jailed for passing data to private eye". *The Age*, 18 September 2019

At the lower end of offending are checks conducted at the request of the friend or relative to provide information about themselves, such as their own driving history or medical records. At a significantly more serious level are instances of access that assist a relative or friend who has links to organised crime activities or that can cause some detriment to a third party. The QPS is particularly at risk with this type of unauthorised access and disclosure (see Chapter 4).

Case study: Employee accessed QPRIME about current partner and ex-girlfriend (QPS)

An administration officer (AOa) inappropriately accessed QPRIME to obtain information about her current boyfriend and his ex-girlfriend and printed out their details. AOa accessed information on QPRIME relating to her boyfriend 24 times and his ex-girlfriend on seven occasions between 1 September and 22 December 2017.

AOa also asked another administration officer (AOb) to undertake a search of the boyfriend on her behalf. This resulted in AOb also inappropriately accessing QPRIME information about AOa's boyfriend.

AOa tendered her resignation prior to any interview being conducted as part of the investigation. On 16 December 2018, AOa was issued with a notice to appear for an offence pursuant to s. 408E of the Criminal Code. On 1 April 2019, AOa pleaded guilty to the offence and was fined $1300 with no conviction recorded. No post-separation disciplinary action was taken.

During the investigation, AOb admitted that AOa had approached her and asked her to access QPRIME in relation to her boyfriend's records. AOb was provided with managerial guidance in relation to her accessing QPRIME at AOa's request.

Conflicts of interest[137] arising from personal relationships have been observed to be a significant corruption risk within QCS. Figure 2 shows that "friendship or personal relationships with prisoners" was the type of conflict of interest most frequently declared by QCS custodial staff. Such relationships may create misplaced loyalty.[138]

137 A conflict of interest arises when a personal interest, such as personal relationship, membership of a special interest group, or financial interest, interferes with an employee's ability to act in the public interest. PSC (2010). *Code of Conduct for the Queensland Public Service*, p. 5. Accessed from https://www.forgov.qld.gov.au/code-conduct-queensland-public-service

138 Submission given by QCS on 10 October 2019 (Submission 1), p. 11

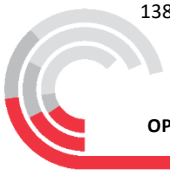
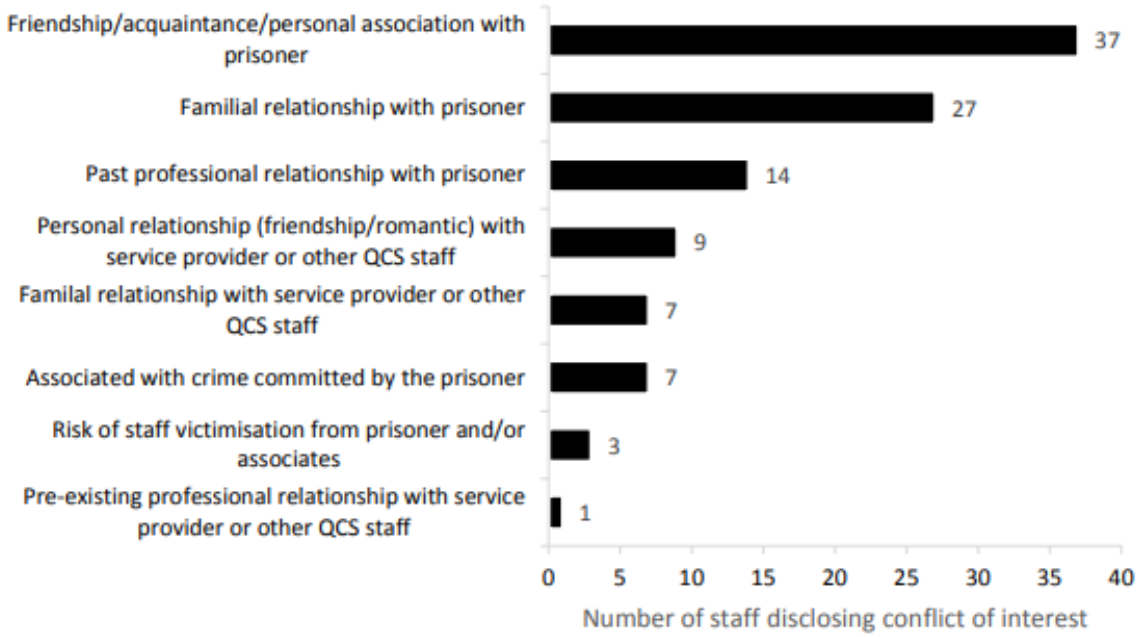


Figure 2: Nature of conflicts of interest declared by QCS staff working in a custodial setting (March to June 2018)



The CCC's Taskforce Flaxton[139] report recommended that QCS implement an "agency-wide electronic system to record conflicts of interest and management action" taken[140] to allow for effective auditing. QCS is yet to implement this recommendation. In relation to this recommendation, Kim Papalia, Assistant Commissioner, Professional Standards and Governance Command, QCS, stated during the hearing that:

> *...it is hard copy reports that we receive, then we enter them on to an Excel spreadsheet database. We would like to move to a platform that is proactively auditable, can provide us greater intelligence capability in terms of linked association and identification of risk. We don't yet have that.*[141]

Considering that inappropriate relationships and associations are a critical corruption risk for QCS, its inability to electronically record such associations to allow for proactive auditing, identification and effective management of association-oriented risks is of concern to the CCC.

139 Taskforce Flaxton examined corruption and corruption risks in QCS.

140 CCC (2018). *Taskforce Flaxton: An examination of corruption risks and corruption in Queensland prisons*, p. 36. Accessed from https://www.ccc.qld.gov.au/publications/taskforce-flaxton

141 Evidence given by Kim Papalia on 15 November 2019, p. 3

Case study: Accessed a relative's records to "check what he was doing" (QCS)

On 7 December 2017, the then Ethical Standards Unit (ESU), DJAG, received a QCS intelligence report relating to an Administration Officer (AO) in a correctional centre. The report indicated that the AO had accessed information on IOMS regarding her son, then disclosed the information she obtained to another officer at another correctional centre. A subsequent audit of IOMS found that the AO had inappropriately accessed her son's information on 62 occasions between November 2012 and November 2017. The information included his offender summary, criminal history, security classification history, case warnings list and employment history. The matter was referred to the Corrective Services Investigation Unit (CSIU) and the CCC on 11 December 2017.

On 23 March 2018, the CSIU advised ESU that the AO would be issued with a notice to appear on a charge for an offence against s. 408E(1) of the Criminal Code. The AO pleaded guilty to the charge on 18 June 2018 and entered into a good behaviour bond. No conviction was recorded.

A subsequent ESU investigation found the allegations of unauthorised access of IOMS information capable of being substantiated and the AO's employment was terminated.

The motivation for the unauthorised access was to check "what he (the AO's son) was doing". The investigation considered that the AO's conduct was "a gross departure from the high standards of conduct expected of a public servant".

Personal circumstances

Employees' personal circumstances may be another motivating factor in misuse of confidential information. These may include drug-related issues, anxiety, broken relationships or the search for new relationships. For example, the issue of police officers using secured databases to obtain information about potential dates has been reported in Western Australia. In February 2019, a former long-serving WA police officer was jailed for six months for improperly accessing the personal details of almost 100 women on the WA police database to determine if they were "suitable" dates.[142]

Case study: Accessed own health records to reduce anxiety (GCHHS)

An Administration Officer (AO) was employed within the Gold Coast University Hospital. The AO accessed information related to herself and her family on 77 occasions. Access was identified through P2Sentinel software, which allowed GCHHS to audit who logs onto the eMR (electronic Medical Records) system. The Queensland Health eMR identifies the surnames of the person accessing the database and the surname of the patient records being accessed. When the surnames match, the system generates a report which is then checked to ascertain if inappropriate access has occurred.

The access occurred in spite of the activities conducted by GCHHS to promote staff awareness about unauthorised access to information; these included Privacy Awareness Week (May 2018), which included warning messages displayed on staff computer screens.

The AO stated the only reason she accessed the records was to see if tests result for herself and referrals for her dependants were in the file, to help reduce her anxiety levels. The investigator outlined numerous Health documents outlining confidentiality requirements for staff when accessing eMR, including the code of conduct, security user responsibility standards, and the clinical records protocol, and AO admitted to understanding some of those.

The AO was issued with a reprimand, and her pay-point was reduced from 3.4 to 3.2.

142 Bell, F. (2019). "Officer jailed for using police database to access personal details of dozens of Tinder dates". ABC News, https://www.abc.net.au/news/2019-02-01/officer-used-police-computer-to-look-up-tinder-dates/10771958, Updated 1 February 2019

Case study: Accessed record of a complaint made by ex-partner (DoE)

The employee was alleged to have inappropriately accessed the details of two complaints made to the department by her ex-fiancé, relating to family court proceedings that she was involved in.
The employee's ex-fiancé alleged the employee inappropriately accessed details of a complaint the ex-fiancé made to the department regarding their son, and that the employee also inappropriately accessed details of a separate complaint made about the complainant's daughter (not related to the employee).
During an assessment of the matter, an audit confirmed that the employee viewed the complaint raised regarding their son on two separate occasions. A further audit by the CCC confirmed that the employee also accessed records relating to the complainant's daughter, including the student's report cards and complaints by the employee's ex-fiancé.

No action was taken against the employee, as she had resigned from the department and the two- year limitation period for considering post-separation disciplinary action, in accordance with s. 188A of the *Public Service Act 2008,* had lapsed

.

Part 3 – Agency frameworks for managing confidential information

This part of the report examines what systems agencies have in place to safeguard their confidential information and to reduce the risk of corrupt conduct relating to unauthorised access and misuse.

Chapter 6 looks at the current information management systems that agencies use to manage access to the confidential information they hold, while Chapter 7 focuses on how agencies can promote an effective information privacy culture.

Chapter 8 looks at possible responses to breaches of confidentiality and the action that agencies, including the QPS, are currently taking in such circumstances.

Chapter 9 explores how public sector agencies can develop and define additional protections to safeguard people's confidential information, including that of vulnerable persons.

Chapter 6 – Organisational systems

Information management and access controls

Access controls are an essential feature of any information management system. Agencies need to have in place robust access control mechanisms to prevent and or reduce unauthorised access to confidential information by employees, and achieve integrity, confidentiality and accountability.[143]

Authentication and authorisation

System authentication and authorisation is the first point of access privilege granted to employees to access agencies' ICT systems. In order for agencies to have knowledge of accesses and operations on their system, a log-on and password are required to get into government ICT systems.[144] The use of unique user identities and passwords in applications also enables audits of employee access to specific databases. Without access data being able to be associated with an employee, access logs may not be traceable, thereby making it extremely difficult for agencies to know the identity of employees who might have engaged in unauthorised access.

Agencies therefore must have the right controls in place to effectively prevent and/or reduce unauthorised access. To achieve this, agencies must implement the Queensland Government Information Security Classification Framework (QGISCF),[145] to classify their data according to its confidentiality level.[146]

Generally, the CCC observed that confidential information on the key databases examined has a unique user identification and password-oriented access.[147] In DTMR's TRAILS/TICA systems, for instance, users first need to log on to the DTMR desktop environment, and then log on again for the TRAILS/TICA system.[148] In deciding whether or not access should be granted to an employee, DTMR applies the "principle of least privilege" to determine access privileges and to ensure that only those people who need to access certain information can do so. During the hearing, DTMR's CIO, Sandra Slater, stated that:

> *So really, that's [access] based on the minimum that you need to do, the role that you need to do…[T]here's a lot of different access levels so that people are restricted to only the data and the functions that they need to do to conduct their work.*[149]

However, analysis of data revealed that, in some of the agencies' other databases, a unique user identification and password were not required to access confidential information. This was particularly so in a significant number of DoE's databases.[150] For instance, although the DoE's spreadsheets contained personal information — including name, home address, passport details, date of birth and place of birth — access to the dataset did not require a unique user identification and password. The implication, as indicated earlier, is that DoE may not be able to trace instances of

143 Cherdantseva, Y., & Hilton, J. (2013). A reference model of information assurance & security. In *2013 International Conference on Availability, Reliability and Security,* p. 552, IEEE.

144 Evidence given by Andrew Mills on 20 November 2019, p. 7

145 See https://www.qgcio.qld.gov.au/documents/information-security-classification-framework-qgiscf

146 Evidence given by Andrew Mills on 20 November 2019, p. 7

147 Agencies' response to CCC's request for information on 6 September 2019

148 Evidence given by Sandra Slater on 11 November 2019, p. 5; see also Exhibit 147

149 Evidence given by Sandra Slater on 11 November 2019, p. 6; see also DTMR's response to CCC's request for information on 21 October 2019, p. 4

150 DoE's response to CCC's request for information on 6 September 2019

unauthorised access to confidential information on those databases, although there may be records of access logs.

Passwords

The issue of password sharing as a corruption risk was of interest to the CCC. Rod Francisco, Executive Director, People, Mackay HHS, noted that Mackay HHS had had a recent case in which an employee shared their password with another employee.[151] Noting that this was a particularly significant problem in the HHSs, Damien Green, CEO of eHealth Queensland, stated during the hearing that:

> *…ieMR has been introduced specifically so that the user must have a dedicated user name and login issue. One of the legacy issues in some Hospital and Health Services was a tendency to share logins for some legacy solutions. Like the emergency department information system, so the information system that many clinicians used to use at the front door of the hospital when they were triaging patients. Some hospitals had a practice of sharing passwords to enable ease of access to the IT system. One of the objectives of implementing the ieMR was to remove that type of practice from the hospital setting.*[152]

The CCC noted that Victoria Police have a system in place which can detect where users have had multiple log-ons and use, which serves as an indication of password sharing. Senior Sergeant Matthew Bell stated that Victoria Police are able to put reports of access logs into a system which can detect simultaneous use of a log-on:

> *We can put those reports into an analyst tool which can spit out where there's simultaneous use on the same system with the same user base. So that is an indication for us of password sharing. Another one may be instances where one person, one user is logged into the actual local network, and then a second user is logged into a system on that same user account.*[153]

User account access review

The main purpose of user account access review is to assess the rights and privileges assigned to employees, ensure that access to confidential information is restricted to those employees who need it, and identify and revoke any unnecessary rights and privileges. Access reviews also have the potential to detect anomalies or unauthorised access to agencies' confidential information.

To this end, a typical user account and access review is able to determine the following:

- unnecessary access rights and privileges that have been assigned to users
- alignment of user accounts with principles of least privilege and separation of duties
- anomalous or unauthorised use of privileged or administrative access rights
- anomalous or unauthorised use of access rights to confidential information or resources.[154]

Analysis of evidence revealed that subject agencies generally conducted user access reviews on the databases that held confidential information, although the approach and frequency of reviews varied. In the case of DTMR, a TRAILS user audit was undertaken every six months to confirm the appropriateness of access provided to employees, in addition to fortnightly reports by HR on exiting

151 Evidence given by Rod Francisco on 12 November 2019, p. 21

152 Evidence given by Damian Green on 14 November 2019, p. 5

153 Evidence given by Matthew Bell on 15 November 2019, p. 6

154 Trusted Information Sharing Network (TISN) (2018). *User-access management: A defence in depth control analysis*, pp. 26-27. https://www.tisn.gov.au/Documents/User-Access+Management++A+Defence+in+Depth+Control+Analysis.doc

staff and staff on extended leave.[155] QCS conducted annual access audits to identify staff who no longer required IOMS access to perform their duties, in addition to quarterly audits to identify staff who had had a change of their access approved.[156] The QPS stated that reviews of this nature were not conducted on their core systems such as QPRIME, as monitoring of user accesses was the responsibility of Officers in Charge at the station level.[157] Acknowledging that this was an area for improvement, the PSBA internal audit team were conducting or were about to conduct a review of corporate access and controls to determine adequacy of compliance.[158]

In some agencies, it was not clear who had the responsibility to monitor and review user access changes to databases holding confidential information. DoH indicated that user access to the ieMR system was managed by individual HHSs, as eHealth Queensland did not manage user access to ieMR production databases[159], while GCHHS noted that it was the responsibility of DoH to monitor user access changes.[160] The CCC observed that eHealth Queensland only conducted monthly access reviews to notify HHSs of employees whose accounts were not active, in order to seek HHSs' approval for removal. The ongoing monitoring and review of user accesses commensurate to employees' roles and duties was therefore the responsibility of HHSs. The CCC noted this was the case with Mackay HHS, as their Digital Hospital Program was responsible for the management, creation and modification of clinical user accounts in line with the schedule of access agreed for different staff.[161] The CCC considers that there is an opportunity for DoH to ensure that there is clarity between the HHSs and DoH regarding who has responsibility for user access reviews.

Access controls for vulnerable persons

It became apparent that vulnerable persons,[162] including domestic violence victims and high-profile people, were particularly susceptible to misuse of their confidential information. Accordingly, public sector agencies needed to identify their own lists of people who fell within this special category in order to provide them with extra protection, including additional control mechanisms and/or flags. The analysis in this section is limited to special access controls relevant to these vulnerable persons.[163]

There were significant variations across agencies in relation to the extra protection required for the confidential information of vulnerable persons. The CCC noted that, in terms of providing additional security or protection to vulnerable persons, DTMR had one of the most progressive systems, their Customer Records Suppression Service.[164] This could be a good model for other agencies to adopt/adapt.

In the case of DoE, Director-General Tony Cook testified during the hearing that there was no system in place that currently provided additional protection to vulnerable persons as DTMR did, although they had the ability to record a court order regarding domestic violence victims.[165]

---

155 DTMR response to CCC's request for information on 21 October 2019, p. 9

156 Submission given by QCS on 10 October 2019 (Submission 1), p. 31

157 QPS response to CCC's request for information on 21 October 2019, p. 5

158 QPS response to CCC's request for information on 21 October 2019, p. 5

159 DoH response to CCC's request for information on 21 October 2019, p. 4

160 GCHHS response to CCC's request for information on 21 October 2019, p. 3

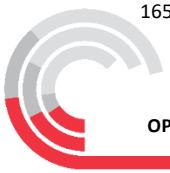
161 Mackay HHS response to CCC's request for information on 21 October 2019, p. 2

162 For the meaning of vulnerable people, see the analysis preceding Recommendation 8

163 See chapter 9 for a detailed analysis of why this category of people needs protection, and a discussion of the use of flags as a detection mechanism for unauthorised access or attempted access.

164 Evidence given by Neil Scales on 11 November 2019, p. 12

165 Evidence given by Tony Cook on 12 November 2019, pp. 27-28



The CCC also noted that an area for improvement for the QPS was to provide additional access controls to protect vulnerable persons, in particular domestic violence victims, which it currently did not do. In the QPS' response to CCC's request for information, it was stated that:

> *QPRIME does not specifically restrict or categorise records relating to vulnerable or high profile persons. This reflects the nature of policing and prevalence of dealing with people who may fall within the vulnerable categorisation. The option exists for notification of attempts to access entities to which ACL [Access Control List] has been applied. This option is exercised on a case by case basis and in certain circumstance such as records relating to covert identities and operations.*[166]

The Commissioner of Police gave evidence that including domestic violence victims on the ACL may restrict the police in effectively providing the needed protection and service to those people and that options needed to be considered on how best additional protection could be provided to domestic violence victims without compromising the efficiency of the police.[167] This view was confirmed by Timothy Dillon, Acting Director, Digital Transformation and End User Tools & Platforms at PSBA.[168]

Recommendation 1 – Access control mechanisms

That agencies:

1. ensure all computer databases where confidential information is stored have unique user identifications log-ons
2. conduct quarterly user access reviews and monitoring of user access changes to help prevent and minimise unauthorised use of these databases
3. ensure additional access control mechanisms are implemented on confidential information of vulnerable people.

Information and data sharing

Effective and timely information sharing[169] arrangements between agencies are needed to promote collaboration and inter-operability. The Queensland Government noted in its 2013–2017 ICT Strategy that information sharing will "reduce duplication and frustration in assessing government services".[170] Section 169A of the *Domestic and Family Violence Protection Act 2012,* for instance, provides for entities to share information, while protecting its confidentiality, in order to:

- assess whether there is a serious threat to the life, health or safety of people because of domestic violence, and
- respond to serious threats to the life, health or safety of people because of domestic violence, and
- refer people who fear or experience domestic violence, or who commit domestic violence, to specialist domestic and family violence service providers.

166 QPS response to CCC's request for information on 21 October 2019, p. 3

167 Evidence given by Katarina Carroll on 18 November 2019, p. 22;

168 Evidence given by Timothy Dillon on 19 November 2019, p. 11

169 The terms "information sharing" and "data sharing" have been used interchangeably in this report.

170 DSITIA (2013). Queensland Government ICT strategy 2013-2017 action plan, p. 20. Access from https://s11217.pcdn.co/wp-content/uploads/2013/08/ict-strategy-action-plan.pdf

During the hearing, information and/or data sharing between public sector agencies was confirmed as critically significant to the effective performance of public sector agencies' functions. The Commissioner of Police, Katarina Carroll, expressed the view that data sharing is critically important for the work of the QPS:

> *…it [data sharing] is critically important for the safety and security of Queenslanders and our officers to share information with other agencies. And in fact, some of the risks and gaps occur if we don't share that information enough or well enough in order to make sure that a victim is protected or, you know, that that community is safe and secure. We have to share information and there are issues if we don't share that information well. It is critical to the success of our organisation and others.*[171]

For this reason, and on the "back of numerous service delivery failures attributed in part to a failure in the effective sharing of information, a need was identified to improve information sharing across Queensland Government".[172] Thus, the QGCIO has developed an information sharing authorising framework (ISAF) to assist public sector agencies in the implementation of a "successful information sharing activity by focusing on the benefits of sharing while managing the risks and understanding the constraints".[173]

Audit of access to shared data

Although memoranda of understanding (MOUs) governing information and data sharing arrangements between agencies clearly state that misuse of shared information is a privacy breach, they are generally silent on the need to audit access to the shared information or data. This is of concern to the CCC, considering the significantly important role of access audits in the detection of alleged privacy breaches.[174]

When asked whether audits were conducted on shared information during the hearing, witnesses from the seven agencies gave responses ranging from "no audits conducted" to "it is the responsibility of the receiving agency", with no clear direction provided in their MOUs. To a CCC request for information in relation to whether shared information was audited, for instance, the QPS responded that:

> *There are no centralised processes to monitor or audit compliance. Compliance with MOU requirements is a matter for the owning Region/Command, and such actions may be dependent on whether there are review, auditing or monitoring clauses within the MOU.*[175]

The QGCIO stated during the hearing that:

> *I would recommend that as good practice that you should actually have some at least confirmation. If you're not handing over and passing that requirement legally to the other side then you would need to audit their requirements.*[176]

---

171 Evidence given by Katarina Carroll on 18 November 2019, p. 15

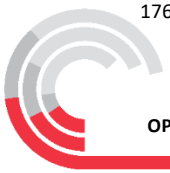
172 QGCIO (2018). Information sharing authorising framework: Comprehensive guidance for information sharing, p. 7. Accessed from https://www.qgcio.qld.gov.au/documents/information-sharing-authorising-framework

173 QGCIO (2018). Information sharing authorising framework: Comprehensive guidance for information sharing, p. 5

174 See chapter 9 ("Improving prevention and detection systems") of this report.

175 QPS's response to CCC request for information on 21 October 2019, p. 6

176 Evidence given by Andrew Mills on 20 November 2019, p. 9



Recommendation 2 – Audit responsibility when sharing data

That public sector agencies ensure MOUs or other agreements which set out the processes and roles in relation to data sharing between agencies contain clauses that specify:

1. which agency is responsible for conducting targeted audits of shared data
2. regularly defined intervals at which audits are to be conducted, preferably quarterly.

Chapter 7 – Promoting effective information privacy culture

An effective culture of information privacy aims to promote ethics and values in relation to its management of confidential information, and takes proactive preventative steps to shape the behaviour of employees. The CCC is of the view that, to achieve this culture, effective policy, education and awareness programs are critically important. This chapter focuses on agencies' relevant policies and educational approaches.

Effective policy

The purpose of policies, procedures and other work instructions is to provide guidance and commentary to employees in relation to their responsibilities and obligations. Policy aims to help employees better understand employer expectations and ramifications for failing to comply with agency standards. The OIC in its submission to the CCC advised that "agencies that collect, use or store personal information should have documented policies in place for managing a privacy breach".[177]

The following key issues were consistently identified as challenges for public sector agencies with regards to creating and maintaining policies in relation to confidential information:

- Confusion regarding what conduct amounts to criminal conduct and what conduct should be dealt with via disciplinary sanction
- Uncertainty regarding the language used to describe the acts giving rise to criminal offending, as opposed to misconduct relating to agency-specific Acts' disclosure provisions regarding confidentiality obligations
- Policies being either silent or difficult to understand in terms of s. 408E offences contained in the Criminal Code or in agency-specific Acts that relate to misuse of confidential information, and
- The decentralisation of responsibility from a lead agency to a smaller entity (in relation to DoH and DoE), creating difficulties in the allocation of resources and approaches to ICT information access policy design and dissemination of standards.

Elements of an effective policy

Clarity and precision

For a policy to be effective in sending the intended message, it needs to be simple and precise. According to Dr Smith, the language used in policies should be simple, clear and accurate; and it may be useful for agencies to generate a single-page factsheet to complement an extended policy to ensure usability and reader understanding.[178] An effective policy can even act as a deterrent for employees by emphasising the certainty of being detected and clarity as to what sanctions might arise.[179]

Acknowledging the importance of a concise, precise policy in building the needed privacy culture within the public sector, the Queensland Teachers' Union in its submission recommended that DoE create clear, practical and comprehensive policies for teachers and school leaders that explain how

177 Submission given by OIC on 9 October 2019 (Submission 2), p. 8.

178 Evidence given by Dr Russell Smith on 11 November 2019, p. 8

179 Rajakaruna, N., Henry, P. J., & Scott, A. J. (2019). Misuse of Police Information Systems: Predicting Perceived Likelihood of Misuse among Unsworn Police Employees. *Policing: A Journal of Policy and Practice*, p. 1; see also exhibit 15

the data they "currently have access to (and specifically data on OneSchool) can be used by them".[180] For instance, although in the DoE's Guideline on Use of ICT Facilities and Devices (the DoE Guideline) there is guidance to staff that a person's confidential information may be accessed with the consent of the involved third party,[181] that same conduct is not acceptable under the Criminal Code unless the access is for a work-related purpose.

Possible examples of "misuse" for inclusion in the DoE Guideline

Example 1

An employee accessing their own personal information on a work computer or work device, whether at work or from a remote location, is unacceptable and may result in criminal and/or disciplinary sanctions.

Example 2

An employee accessing a family member's confidential information for a purpose other than one that is work-related, despite having the consent of the family member to conduct the enquiry, is unacceptable and may result in criminal and/or disciplinary sanctions.

The CCC noted that DTMR's Access to Customer Records policy is concise and precise in terms of covering the key definitions and practical examples of what constitutes authorised access and unauthorised access and could be a good model for other agencies, such as DoE, to adopt and/or adapt.

Clear enunciation of consequences

Evidence revealed that ambiguity about the possible sanctions for misuse of confidential information could have a negative impact on promoting the required privacy culture in agencies. For this reason, it is important to explain the range of sanctions available in the event of wrongdoing.[182] The CCC advises agencies to make it clear in their policies and other media that "where computer hacking and misuse by a public officer results in a breach of a citizen's privacy, the public interest will almost always require prosecution".[183] During the hearing, Tony Cook, Director-General of DoE, readily acknowledged that it would be beneficial to staff to be informed of the entire range of possible sanctions that might arise by breaching privacy.[184]

One way of informing employees is to have policy and procedure documents include cases where sanctions have been applied. This was particularly emphasised by Dr Smith during the hearing:

> *…research has found that people often don't believe that there are [sanctions] going to be applied to them individually. It's very difficult to make people understand that a range of potential sanctions will eventually be applied to them if they do the wrong thing. So ways around that problem are to demonstrate cases where sanctions have been applied, case studies where cases have gone to court, people have received terms of imprisonment or serious fines, and people can then see that the sanctions are in fact applied.*[185]

---

180 Submission given by Queensland Teachers Union on 9 October 2019 (Submission 6), p.4.

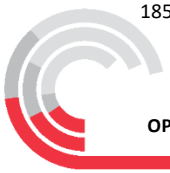
181 S. 426(4)(b) of the Education Act.

182 Evidence given by Dr Russell Smith on 11 November 2019, p.8.

183 CCC (2019). Improper access to public sector databases, no. 2, p. 3. Accessed at https://www.ccc.qld.gov.au/sites/default/files/Docs/Publications/CCC/Prevention-in-Focus-Improper-access-to-public-sector-databases-no2-2019.pdf

184 Evidence given by Tony Cook on 12 November 2019, p.15.

185 Evidence given by Dr Russell Smith on 11 November 2019, p.8.



Use of de-identified case studies

Case studies can be a useful mechanism for putting examples of appropriate and inappropriate use of confidential information in context for employees, and can be used in training and awareness programs. To achieve the intended deterrent effect, Dr Smith advised that cases would need to include sufficient detail about the facts of the matter, the personal circumstances of the individual(s) involved and the sentencing considerations, to enable the community to understand the decision reached regarding sanctions.[186]

Managing decentralisation

It is important for agencies such as DoE and DoH to lead their smaller, devolved entities. Dr Smith told the CCC that, very often, smaller entities were not equipped with the same resources to develop individualised policy.[187] Best practice necessitates that lead agencies make available policy templates, in addition to accompanying guidance, to show how the standard templates might be adapted to suit the needs of a given HHS or school.[188] The lead agency ought to monitor and review the development of smaller entities' policy, which will help ensure consistency of general principles and standards across the relevant sector.[189]

Recommendation 3 – ICT Information Access Policy

3.1 That all public sector agencies develop a comprehensive and concise ICT Information Access policy. The policy should refer to the Criminal Code, the relevant public sector agency governing Act and the IP Act. It is critical that language used is standardised to ensure consistency and better understanding. In particular the policy should include for each of these three Acts:

1. the meaning of confidential information
2. the meaning of unauthorised use
3. the meaning of unauthorised disclosure
4. the range of potential sanctions including criminal charges and disciplinary proceedings, such as termination, demotion, and/or the imposition of a post-separation declaration, and
5. de-identified case studies of substantiated allegations relating to the misuse of confidential information and the consequences of those matters for the employee.

3.2 That public sector agencies with decentralised agencies (for example, Queensland Health and the Department of Education) provide sufficient support to ensure that the decentralised agencies have comprehensive and concise ICT Information Access policies in place. Sufficient support includes, but is not limited to:

1. providing templates, and
2. reviewing the policies implemented by decentralised agencies annually.

186 Evidence given by Dr Russell Smith on 11 November 2019, p. 9.

187 Evidence given by Dr Russell Smith on 11 November 2019, pp.10-11.

188 Evidence given by Dr Russell Smith on 11 November 2019, p. 11.

189 Evidence given by Dr Russell Smith on 11 November 2019, p. 11.

Education and awareness

An important part of public sector integrity systems is prevention. The main objective of any prevention strategy is to identify and prevent corruption risks being realised in the first place. The significant number of information breaches that occur internally within organisations highlights the importance of understanding how agencies can proactively work to reduce such behaviour.[190] A clear understanding and awareness of information privacy requirements and the associated consequences when a breach occurs is therefore critical for promoting compliance. The ISO/IEC 27001:2015 standard includes awareness, education and training as preventative approaches that organisations need to implement.[191]

It is evident that education and awareness have a significant positive impact on the information privacy culture of organisations.[192] The OIC advises that in order for agencies to establish good privacy practices, procedures and systems, they need to promote privacy awareness by incorporating information privacy education into training programs.[193] This section examines the education and awareness programs conducted by the subject agencies to identify strengths and gaps requiring improvement across the entire Queensland public sector.

Training and assessment

An effective training and assessment program is critical for promoting information privacy culture within organisations. Some agencies have a relatively strong training program in place (for example, DTMR and Mackay HHS), whereas others, such as the QPS, had a somewhat less robust approach to training. Table 2 shows that the QPS does not provide regular training to staff regarding QPRIME, the information system that contains its most valuable confidential information. It was also evident that the QPS does not provide regular training regarding information privacy, ethics and information security.[194] For instance, during the hearing, a corruption investigation involving a QPS officer was discussed. The investigation was in relation to unauthorised access to confidential information. The alleged conduct occurred in 2016 and as at 2019, when the matter was finalised, the most recent training undertaken by the officer (QPS's Ethics and Ethical Decision Making training module) had been completed in 2015.[195] There had been a period of four years where the officer had not undertaken relevant training. The frequency of training was readily acknowledged by Sharon Cowden, Assistant Commissioner, Ethical Standards Command, as an area of improvement for the QPS.[196]

It was also evident that training regarding QPS information systems such as QPRIME was restricted to sworn officers during recruit training.[197] This is in sharp contrast to a recent finding that training regarding the appropriate use of information systems should not be restricted to only sworn officers

190 Da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security*, 49, p. 162

191 ISO/IEC 27001:2015. Information technology – security techniques – information security management systems – requirements, p. 9

192 Da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security*, 49, p. 174

193 OIC (2018). *Awareness of privacy obligations: How three Queensland government agencies educate and train their employees about their privacy obligations*, p. 1

194 See Exhibit 104. Accessed from https://www.ccc.qld.gov.au/public-hearings/operation-impala

195 See Exhibit 120

196 Evidence given by Sharon Cowden on 18 November, p. 12

197 See Exhibit 120

but must include both sworn and unsworn officers.[198] Training that specifically relates to information privacy and the appropriate use of information systems should be mandatory for all employees.[199]

Table 2: Subject agencies' training[200]

Agency	Information system	Period undertaken following employment	Mode of delivery	Frequency of on-going training
QPS	QPRIME	By week two of recruitment training	Face-to-face	Not applicable
QCS	IOMS	Yes	Online and face-to - face	Varies – depends on role
DoE	OneSchool	No mandatory requirement to train – localised business decision by the school	Online or face to face	Yes (on as needs basis)
DTMR[201]	TRAILS/TICA	Prior to access	Online	Yes (two yearly)
DoH[202]	ieMR	Managed by HHSs	Managed by HHSs	Managed by HHSs
GCHHS	ieMR	Prior to commencement	Face-to-face and online	Yes (annual)
Mackay HHS	ieMR	On commencement	Face-to-face, online, classroom	Yes (two-yearly)

The critical need to provide effective training for employees regarding issues of information privacy, especially in relation to the use of agencies' information systems that contain confidential information, was acknowledged by the QNMU, QPUE and QTU. In its submission, the QTU stated that following the creation of clear, practical and comprehensive policies, procedures and guidelines for teachers and school leaders that clarified the purpose for which data may be accessed on OneSchool, "extensive training should be provided to all State School teachers and school leaders by the Department of Education" and should be updated annually.[203]

In the public hearing, Ian Leavers, QPUE, emphasised the importance of training and education to QPS officers as an important approach to preventing unauthorised access to and disclosure of confidential information, especially on QPRIME, as officers are sometimes not aware of what they can and cannot access:

198 Rajakaruna, N., Henry, P. J., & Scott, A. J. (2019). Misuse of Police Information Systems: Predicting Perceived Likelihood of Misuse among Unsworn Police Employees. *Policing: A Journal of Policy and Practice*, p. 11

199 Evidence given by Dr Russell Smith on 11 November 2019, p. 7; see also submission given by OIC on 9 October 2019, par 14.

200 Agencies' response to CCC request for information on 6 September 2019. This table is a summary of training provided by agencies to employees. Many agencies also provide other training to staff which is not specific to the particular database listed in the table, but educates staff in relation to privacy responsibilities and when it is appropriate to access official records.

201 DTMR provided further examples of training which is provided to customer staff in its original submission to the CCC and in its response to the draft report.

202 DoH's unawareness of the happenings in HHSs is of concern to the CCC and reiterates the need for lead agencies to monitor, from time to time, the activities of HHSs. This is discussed in detail in the section "Decentralised agencies".

203 Submission given by QTU on 9 October 2019 (Submission 6), p. 28

> *I think we need to have a good training package so people can fully understand this. Because I do not believe people go to work each and every day thinking I'm going to access the QPRIME system so I can commit an offence or deliberately do something wrong. That is not the nature of police. And police don't know what they can or cannot do at this point in time.*[204]

During Operation Impala, four key aspects of training emerged as critically important for building and promoting the requisite organisational information privacy culture: the content of training, the frequency of training, the mode and assessment of training, and the need for consistency across decentralised agencies.

Content of training

For training to be effective, it must cover all the necessary components and be both accurate and relevant for the intended purpose.[205] Necessary components include, but are not limited to, information privacy requirements, business controls and legal responsibilities. Training should alert staff to relevant policies and possible consequences for unauthorised access to confidential information, including disciplinary action and criminal prosecution. De-identified case studies should be used to illustrate consequences. This method of training emerged as one of the most effective in the course of the public hearing.[206] The use of de-identified case studies as a critical component of agencies' information privacy training was strongly endorsed by Dr Smith during the hearing.[207]

This is consistent with a recent finding that when employees are certain that they will be punished for breaching information privacy, they are less likely to engage in unauthorised access and disclosure of confidential information.[208] The CCC notes that an effective training package that covers all relevant components is an area for improvement in some subject agencies (QCS, DoE and QPS). QPS information privacy training does not specifically outline the range of disciplinary sanctions that could be applied, including the possibility of instituting criminal charges under s. 408E of the Criminal Code, where breach of privacy occurs.[209] Sharon Cowden, QPS Ethical Standards Command, stated that QPS's current training package had been in place since 2016, and that she recognised the need to have appropriate training and awareness in place.[210]

Frequency of training

Table 2 shows that agencies generally provided training to employees regarding access to their information systems. However, a number of agencies did not provide regular compulsory refresher training to staff. The QPS only provided training upon request and there was no regular training provided to employees in relation to some critical areas, such as the use of QPRIME and QLiTE, and privacy awareness, information security and ethics and ethical decision making.[211] Ms Cowden acknowledged that training could be better, in terms of offering regular mandatory training to employees to build and promote the requisite information privacy culture in the QPS and the Queensland public sector more broadly:

---

204 Evidence given by Ian Leavers on 18 November 2019, p. 8

205 OIC (2018). *Awareness of privacy obligations: How three Queensland government agencies educate and train their employees about their privacy obligations*, p. 23

206 Evidence given by Rachael Rangihaeata on 22 November 2019, p. 14

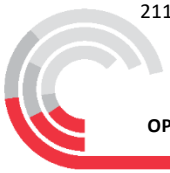
207 Evidence given by Dr Russell Smith on 11 November 2019, p. 8

208 Rajakaruna, N., Henry, P. J., & Scott, A. J. (2019). Misuse of Police Information Systems: Predicting Perceived Likelihood of Misuse among Unsworn Police Employees. *Policing: A Journal of Policy and Practice*, p. 11

209 QPS response to CCC request for information on 21 October 2019, Attachment 1

210 Evidence given by Sharon Cowden on 18 November 2019, p. 12

211 Exhibit 104 and also QPS response to CCC request for information on 6 September 2019



> *…when we answered some of the questions for the Commission, and sent our responses through, we had some honest conversations at that, sort of, executive level saying, "Well, this is useful because we've got some gaps here". One of the things that is already in play is a development of an online learning – a new online learning package… so we will, in 2020, have a new online learning product. That is my intention… [and] we will mandate that as well.*[212]

Dr Smith suggested that training should be provided to employees upon commencement of employment, before being granted access to confidential information, and that refresher training must be provided at least every two years. This could be more regular, particularly when the risk associated with the misuse of confidential information was relatively high.[213]

It is important that training completed by staff is captured by agency records. In the course of the public hearings, it became evident that details of training conducted and training participants were not adequately recorded. Absence of training records makes it difficult for agencies to track participants and gauge staff awareness. This presents a significant risk for the identified agencies and the entire Queensland public sector, particularly in circumstances where employees are subject to internal investigations. To mitigate this risk, public sector agencies should take appropriate steps to ensure that training undertaken, and details of training participants, are captured by agency record management systems.

Mode and assessment of training

Dr Smith advised that effective training should be a combination of online and face-to-face modules, with face-to-face as the preferred option where resources and capacity allow.[214] Thus a scenario-based training system is required to build the information security culture[215]; face-to-face training is particularly beneficial for this form of training. This position was also supported by the Commissioner of Police, who stated that information privacy training should be multifaceted, including a combination of online and face-to-face options. She noted that a face-to-face learning option is incredibly important.[216] Similarly, Dr John Wakefield, the Director-General of DoH stated that from his own "experience and expertise in human factors, the strength of the control is much better with face-to-face training than it is in terms of online" or any other mode of delivery.[217]

Further, Dr Smith indicated that for a training and education program to be effective, it should be evaluated to ascertain the level of understanding employees have regarding the need to comply with information privacy requirements and whether the content of the training is actually targeting the outcomes agencies hope to achieve.[218] Da Veiga (2016) found that the information security culture of employees who actually read and understood the information security policy of their agency was significantly higher than those who did not understand.[219]

---

212 Evidence given by Sharon Cowden on 18 November 2019, p. 12

213 Evidence given by Dr Russell Smith on 11 November 2019, p. 5-6; see also See also evidence given by Dr John Wakefield on 14 November 2019, p. 31-32; IBAC (2019). *Unauthorised access and disclosure of information held by Victoria Police*, p. 28-29; OAIC (2015). *Privacy management framework: enabling compliance and encouraging good practice*, p. 4.

214 Evidence given by Dr Russell Smith on 11 November 2019, p. 5

215 Evidence given by Ian Leavers on 18 November 2019, p. 8

216 Evidence given by Katarina Carroll on 18 November 2019, p. 38, 67; see also evidence given by Rachael Rangihaeata on 22 November 2019, p. 14-15

217 Evidence given by Dr John Wakefield on 14 November 2019, p. 13

218 Evidence given by Dr Russell Smith on 11 November 2019, p. 7

219 Da Veiga, A. (2016). Comparing the information security culture of employees who had read the information security policy and those who had not: Illustrated through an empirical study. *Information & Computer Security*, *24*(2), p. 149

Decentralised agencies

Lead agencies, such as DoE and DoH, each with several devolved agencies, sometimes experience inconsistencies in the areas of training and the content of policy and procedure documents. This issue becomes even more complex when some devolved agencies such as HHSs are themselves statutory bodies with their own independent Boards. Mackay HHS, for example, uses de-identified case studies as part of their training as an effective way of building the requisite information privacy culture among employees;[220] however, GCHHS does not, although Hannah Bloch acknowledged it "would be a very valuable tool".[221] Evidence across the board revealed that it was an important step forward for lead agencies to set a framework that established guidelines and protocols for devolved agencies to adopt or adapt.[222] Dr Smith stated during the hearing that:

> *There should be some monitoring by the central agency about what's taking place so that you don't have a smaller part of the department preparing its own material that is slightly incorrect or doesn't follow the general principles that have been outlined.*[223]

Recommendation 4 – Confidential information access and privacy training

4.1 That agencies ensure that training:

1. is developed and provided to all public sector employees prior to gaining access to any database that contains confidential information
2. is developed and provided annually to all public sector employees who have access to confidential information
3. reflects the respective ICT access and use policy, including references to the Criminal Code, the relevant public sector agency governing Act and the Information Privacy Act. The language used in the training material should be consistent and include explanation of items numbered 1 to 5 outlined in Recommendation 3.1
4. comprises a combination of online, face-to-face and video modules
5. records of the content and participation by employees are kept
6. is assessed annually to determine levels of retention and understanding of the content of the respective Information Privacy policy and supporting training material.

4.2 That public sector agencies with decentralised workforces (for example, Queensland Health and the Department of Education) provide sufficient support to ensure that the decentralised agencies conduct all-inclusive training. Sufficient support includes, but is not limited to:

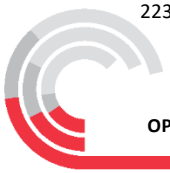
1. providing guidelines, and
2. conducting an annual review of the decentralised agencies' training.

220 Evidence given by Rod Francisco on 12 November 2019, p. 7

221 Evidence given by Hannah Bloch on 13 November 2019, p. 10

222 Evidence given by Dr John Wakefield on 14 November 2019, p. 20

223 Evidence given by Dr Russell Smith on 11 November 2019, p. 11



Awareness

Employees' awareness of information privacy requirements and the possible consequences of a breach has been acknowledged as a critical factor in promoting information security and a privacy culture in agencies.[224] Employees' awareness of the certainty of detection and punishment significantly reduces their intention to misuse confidential information and thereby creates the requisite information security and privacy culture in agencies.[225] There are three components that are critical to creating the requisite awareness: communication by leadership; log-on warnings, screensavers and posters; and toolbox talks, newsletters and de-identified case studies. The CCC noted that DTMR and GCHHS had quite robust information privacy awareness campaigns. For example, GCHHS commenced a privacy awareness campaign in the beginning of 2019 as a response to the steep increase in information privacy breach allegations and intended to make it an ongoing campaign:

> *…we particularly tailored the message around access to your own information and the potential consequences insofar as criminal referrals to the police, potential therefore [for] imprisonment or whatever the outcome may be, disciplinary action etc. So we really tailored the messaging in that program around not looking at your records just as much as treating records appropriately… We actually have a new program that we're about to release which is where the catchphrase is "Our lips are sealed", so we're going to roll out a new wave of messaging for staff around the importance of confidentiality… So that will include posters, blogs, lip gloss for staff that has got clearly marked on it "Our lips are sealed" to hand out to staff… So we will use all of those tools to be able to remind staff of the importance of confidentiality.*[226]

Similarly, since 2017, DTMR has developed annual campaigns, such as "A Peek is a Breach" (see Appendix 3) which aims to raise awareness of the need for employees to comply with information privacy requirements and includes emails, videos, posters and toolbox talks.[227]

Communication by leadership

In public integrity and anti-corruption efforts, it is commonly acknowledged that the tone is set from the top – meaning leadership is overwhelmingly critical if anti-corruption efforts are to be successful.[228] In order to build information privacy culture within public sector departments, leadership resolve to send the right message on the necessity for information privacy compliance should be an ongoing practice.[229] To this end, leadership plays a critical role in the establishment of an effective information privacy culture.[230] Numerous witnesses gave evidence in relation to the importance of organisational leadership. For example, the issuing of agency-wide directives, by email, would illustrate strong leadership which could filter through an entire organisation. Directives

---

224 CCC (2018). Improper access to public sector databases: What you should know, p. 3. Accessed from https://www.ccc.qld.gov.au/sites/default/files/Docs/Publications/CCC/Prevention-in-Focus-Improper-access-to-public-sector-databases-2018.pdf

225 Kuo, K. M., Talley, P. C., Hung, M. C., & Chen, Y. L. (2017). A deterrence approach to regulate nurses' compliance with electronic medical records privacy policy. *Journal of medical systems*, *41*(12), p. 1; see also D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), p. 94

226 Evidence given by Hannah Bloch on 13 November 2019, p. 8-9

227 Evidence given by Geoffrey Magoffin on 20 November 2019, p. 9-10

228 See, for example, Ankamah, S. S., & Manzoor E Khoda, S. M. (2018). Political will and government anti-corruption efforts: What does the evidence say?. *Public Administration and Development*, *38*(1), 3-14.

229 Ankamah, S. S., & Manzoor E Khoda, S. M. (2018), Political will and government anti-corruption efforts: What does the evidence say? *Public Administration and Development*, *38*(1), p. 4

230 OIC (2019). *Information Management: Queensland government department maturity*. Report No.2, p. 1. Accessed from https://www.oic.qld.gov.au/__data/assets/pdf_file/0008/38708/report-audit-of-information-management-maturity.pdf

from agency leaders would contribute to building and promoting a corruption-resistant information privacy culture. This evidence is summarised by the OIC and HRC respectively:

> *Higher levels of information management maturity require active engagement across a department. Champions at a senior level must lead this change, demonstrating how the agency values, manages and shares information and data appropriately, and how respective business units contribute.*[231]

> *A genuine commitment to this approach [information privacy culture] cannot be achieved through policy alone. Policies need to be supported by understanding and leadership from senior officers, and training for all staff.*[232]

Log-on warnings, screensavers and posters

Log-on warning signs on databases holding confidential information were commonly referred to as one of the tools that agencies could use to promote a strong information security culture. It was evident that agencies generally had log-on warning messages that staff saw prior to accessing agencies' restricted computer databases. However, a number of these messages do not articulate the range of consequences that may result from unauthorised access to databases. Effective warnings should include the attributes stipulated in table 3. Further, Dr Smith suggested that for a log-on warning message to be effective in carrying the intended deterrent message to employees, it needs to be regularly modified and employees' knowledge of the content of the message needs to be regularly assessed.[233]

Table 3: Attributes of log-on warning messages recorded on TRAILS/TICA, QPRIME and IOMS [234]

Agency	Information system	Attributes		
		Unauthorised access is prohibited	Access is monitored	Breach may result in disciplinary sanction and possible criminal charges
DTMR	TRAILS/TICA	Yes	Yes	No
QPS	QPRIME	Yes	Yes	Partially
QCS	IOMS	Yes	Yes	Yes

231 Submission given by OIC on 9 October 2019 (Submission 2), par 15; evidence given by Rachael Rangihaeata on 22 November 2019, p. 16

232 Submission given by HRC on 3 December 2019 (Submission 11), par 27

233 Evidence given by Dr Russell Smith on 11 November 2019, p. 7

234 See Exhibits 79, 135 and 147

Computer screensavers and posters with warning messages about the misuse of confidential information and possible consequences are another form of creating awareness of and promoting information privacy culture within agencies. However, the CCC observes that, like log-on warning messages, information on screensavers and posters should be concise in terms of containing relevant information about the monitoring and auditability of access to restricted computer databases in order to identify potential breaches; and the range of consequences, both disciplinary and criminal, that may be applied. The CCC further notes that, like log-on warning messages, screensavers and posters should be regularly modified to stay relevant for their intended purpose.

Log-on warnings from some agencies, such as DoE and HHSs, could also highlight that the impact of misusing confidential information could adversely affect their professional registration. In many instances breaches of this nature are also required to be reported to other professional regulatory bodies such as, for registered health practitioners, the Office of the Health Ombudsman.

Toolbox talks, newsletters and de-identified case studies

The use of toolbox talks was shown to have the potential to build and promote information privacy culture within agencies. These talks enable business units to come together periodically, mostly monthly or quarterly, to discuss important issues such as information privacy compliance and the range of possible consequences of breaches. The use of toolbox talks in information privacy awareness was demonstrated by agencies such as Mackay HHS, DTMR and GCHHS. In the case of Mackay HHS, de-identified case studies were used to drive the discussions in such talks.[235] In the CCC's view, the use of de-identified case studies is one of the most effective ways to create awareness of acceptable and unacceptable employee conduct within agencies.[236] This position was supported by expert witness Sarala Fitzgerald, a Victorian human rights barrister, who stated that there is a:

> *…very strong public interest in police training and in the training of police prosecutors using real life information, just because those kind of real life examples are always a much more accurate training tool than the sort of cardboard examples that can be thought up by examiners…*[237]

Another means by which agencies could raise awareness is including de-identified cases studies in their monthly newsletters or bulletins. Since February 2019, the QPS has published monthly bulletins on employee disciplinary outcomes, which include breaches regarding information privacy. This approach adopted by the QPS supports earlier findings that employees' perceptions on the certainty of punishment for misuse of confidential information has a positive deterrent effect.[238]

235 See text preceding Recommendation 2 for discussion on the use of de-identified case studies under the heading "Elements of effective policy".

236 Alan MacSporran QC, found in evidence given by Rod Francisco on 12 November 2019

237 Evidence given by Sarala Fitzgerald on 19 November 2019, p.16.

238 Rajakaruna, N., Henry, P. J., & Scott, A. J. (2019), Misuse of Police Information Systems: Predicting Perceived Likelihood of Misuse among Unsworn Police Employees. *Policing: A Journal of Policy and Practice*, p. 11

Recommendation 5 – Privacy awareness messaging

That public sector agencies undertake regular information privacy awareness campaigns including but not limited to:

1. annual email messaging to all employees by the Commissioner, Director-General or Chief Executive Officer to communicate the agency's position clearly as regards information privacy, including acceptable and unacceptable conduct
2. bi-annual email messaging of same to employees by senior executive officers
3. screensavers and posters that stipulate the consequences of misusing a restricted computer database [see items 1 to 5 of Recommendation 3.1], to be updated on a quarterly basis
4. log-on warnings displayed before accessing a restricted computer database to remind public sector employees that access is logged and monitored and that consequences of misuse of confidential information may result in criminal charges under s408E of the Criminal Code and/or disciplinary sanctions, and
5. de-identified case studies—for example, for inclusion in monthly newsletters or for discussion during toolbox talks.

Chapter 8 — Dealing with allegations regarding misuse of confidential information

This chapter begins by examining the current practices of agencies in dealing with allegations of misuse of confidential information. As previously stated, allegations of this nature can lead to both criminal and disciplinary proceedings. Although individual agencies are responsible for taking appropriate disciplinary action against their own employees, the responsibility to commence criminal proceedings rests with the QPS.

This chapter looks at some of the reasons given by agencies for not referring allegations of information misuse to the QPS. It also explores the potential risks of undertaking a disciplinary investigation before referring matters to the QPS. It then looks at whether agencies have been dealing with disciplinary matters in a consistent manner and some of the reasons why this may not be occurring. It then sets out what steps agencies and the QPS should adopt to ensure consistent approaches to referring criminal matters to the QPS and achieve a more consistent approach to dealing with disciplinary matters.

As with other chapters in this report, the CCC determined not to report the approach of every agency examined during Operation Impala, but rather to draw upon examples from a selection of agencies to demonstrate areas for improvement across the public sector.

Current approach by agencies

Public sector agencies are required to report instances of suspected corrupt conduct by their employees to the CCC, and are actively encouraged by the CCC to refer potential criminal matters to the QPS. Information obtained from the subject agencies demonstrates that there are differing approaches to dealing with misuse of confidential information across the public sector.

Key issues identified

The primary challenges for agencies in dealing with breaches may be summarised as follows:

- Ascertaining when to deal with allegations of misuse of confidential information in the disciplinary arena alone, and the circumstances in which allegations should be referred to the QPS.
- Ensuring that consistent disciplinary outcomes are provided by agencies in response to breaches.
- Minimising the risks associated with disciplinary processes occurring prior to allegations being reported to the QPS for consideration of criminal charges.

To maintain public trust and confidence in the public sector, agencies are to deal with misuse of confidential information in a way that is consistent, efficient and appropriate. Agency responses that are effective and timely, and consistently commensurate to the type of offending, will likely improve employee understanding, reduce breach occurrences and mitigate the risks of harm that follow.[239]

239 Evidence given by Dr Russell Smith on 11 November 2019, pp. 8-9, and having regard to exhibit 15, a research article by Rajakaruna, N., Henry, P., & Scott, A. (2019), Misuse of Police Information Systems: Predicting Perceived Likelihood of Misuse Among Unsworn Police Employees, Oxford University Press, pp. 1-15.

When is misuse of confidential information a criminal offence?

It is the view of the CCC that when agencies are made aware of an allegation that one of their employees has misused confidential information from their databases, the starting point should always be that the matter is serious and should be considered for referral to the QPS for criminal investigation. The CCC regularly communicates this view to agencies in referral correspondence[240] and also through publications:

> *Where computer hacking and misuse by a public officer results in a breach of a citizen's privacy, the public interest will almost always require prosecution. Agencies who detect such conduct by their staff should ensure that criminal prosecution is seriously considered – this will generally require the matter being referred to the QPS as a criminal complaint.* [241]

Three main factors were identified as determining why some agencies regularly referred allegations of misuse of confidential information while others did not:

- The degree of knowledge and understanding of when particular types of conduct fall within the criminal offence of computer hacking and misuse (s.408E)
- Agencies putting too much emphasis on the particular personal circumstances of the employee
- The perception by agencies that the QPS considers "lower level" computer hacking and misuse allegations as not being in the public interest to prosecute.

Agency decision making – referrals to the QPS

One of the issues explored by the CCC was the frequency with which agencies referred allegations of misuse of confidential information to the QPS for consideration of criminal charges. The CCC was interested in understanding why some allegations of this type, which could have been referred to the QPS, were not.

Obstacles to referral

Where an agency refers an allegation of misuse of confidential information to the QPS for investigation, the offence ordinarily often considered for charging is s. 408E of the Criminal Code (computer hacking and misuse).

The meaning of some terms in s. 408E — such as "computer hacking" and "benefit" — has proven to be particularly challenging for agencies when determining what action to take against an employee suspected of having misused confidential information. The discussion below is centred on agencies' understanding and interpretation of the term "benefit". (Further discussion of this term, and of other elements of this offence, can be found in chapter 10.)

240 Letter CCC to GCHHS dated 2 April 2019 (Exhibit 58).

241 CCC (2019). *Improper access to public sector databases, no. 2*, p. 3. https://www.ccc.qld.gov.au/sites/default/files/Docs/Publications/CCC/Prevention-in-Focus-Improper-access-to-public-sector-databases-no2-2019.pdf (Exhibit 89).

Understanding the meaning of "benefit"

It is an offence under s. 408E of the Criminal Code merely to access confidential information without a work-related purpose[242]; if a benefit is obtained, the conduct is considered aggravated, thereby attracting a harsher penalty.[243] Importantly, "benefit" includes a benefit obtained by or delivered to any person.[244] The net is widely cast in terms of the type of benefit, and is not confined to financial or personal benefit and may include mere knowledge alone:[245]

> *"**benefit**" includes property, advantage, service, entertainment, the use of or access to property or facilities, and anything of benefit to a person whether or not it has any inherent or tangible value, purpose or attribute.*

An agency's, or individual decision maker's, understanding and interpretation of the term "benefit" will affect their decision on whether or not to refer an allegation of misuse of confidential information to the QPS for consideration of criminal charges. Few of the decision makers within agencies are lawyers, or have a thorough knowledge of the jurisprudence with respect to s. 408E, and so may find it difficult to determine whether an employee's conduct in accessing or disclosing confidential information meets the legal definition of "benefit" as set out in the Criminal Code.

The CCC examined case studies from different agencies, which highlighted some of the complexities involved in determining whether a benefit was obtained by the employee who improperly accessed the confidential information:

- The information obtained by the employee did not benefit the employee themselves, but some other person to whom it was communicated.
- The information obtained (the benefit) could have been lawfully obtained by the employee through another lawful avenue.
- The benefit obtained by the employee was limited to the information accessed, that is, there was no extrinsic benefit such as money or other property as a result of accessing the information.

In some cases examined by the CCC, the reasons cited above were used to not refer the matter for criminal prosecution. The CCC's view is that in all these instances the employee who accessed the information improperly obtained a benefit as defined in the Criminal Code.

During the Operation Impala public hearings, discussion was had during the evidence of Geoffrey Magoffin, Customer Service General Manager at DTMR, about five previous cases that had not been referred by DTMR to the QPS for consideration of criminal charges. In discussing these matters with Mr Magoffin, the CCC noted that he was a decision maker only in relation to disciplinary matters for staff under his control[246], and that he did not determine which matters DTMR as a whole referred to the QPS for consideration of criminal charges.[247] The aim of the discussion with Mr Magoffin was to explore how he determined appropriate disciplinary sanctions in cases where he was the decision maker and, in relation to the other cases, any reasons he could give, to the extent he was able, for matters not being referred to the QPS by other DTMR decision makers.

---

242 Criminal Code, s. 408E (1) (Exhibit 11), the relevant wording in that section is expressed as being "for a legitimate business reason".

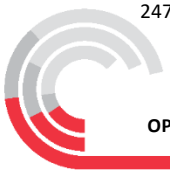
243 Ibid, s. 408E (2).

244 Ibid, s. 408E (5).

245 Criminal Code, s. 1 (Exhibit 108); Police and Daniel Denis Banks, decision at Ipswich Magistrates Court on 15 September 2017, p. 3 (Exhibit 155).

246 Evidence given by Geoffrey Magoffin on 20 November 2019, p. 20

247 Evidence given by Geoffrey Magoffin on 20 November 2019, p. 38



The role of the CCC

The CCC has a role in assisting agencies identify matters which are serious and ought to be referred to the QPS for consideration of criminal charges.[248] Consequently, to assist agencies in their understanding of the term "benefit" and the circumstances in which an employee's conduct may constitute a criminal offence, the CCC records, analyses, assesses and reviews complaints of corruption to help inform, educate and empower agencies to reduce corrupt conduct.

The CCC assesses every complaint it receives to decide how serious it is, whether it warrants investigation, how quickly it must be actioned and who is best placed to investigate it. Based on the assessment, the CCC may decide to take no further action; investigate the complaint itself; refer the complaint to the agency to deal with, subject to CCC oversight; conduct a joint investigation with the agency; and/or refer possible criminal activity to the police.

Investigations subject to CCC oversight are monitored by the CCC.[249] Factors determining whether a matter is referred to an agency subject to monitoring include the seriousness and/or systemic nature of the allegation/s, whether the nature of the allegation/s is an area of focus for the CCC, and the confidence the CCC has in the agency to deal with the matter appropriately.

Throughout the monitoring process, review officers from the CCC will monitor the compliance of an agency with stipulated timeframes and reporting requirements. These CCC review officers are also available to provide advice and guidance to agency liaison officers and investigators in how to conduct investigations into allegations of corrupt conduct, such as misuse of information.

Additionally information is available on the CCC website via corruption prevention publications and in Corruption in Focus, a guide designed to help agencies assess and investigate allegations of corrupt conduct.

In addition, the CCC has published corruption prevention papers on misuse of confidential information, and the role of prosecution and disciplinary action:

- *Corruption in the public sector – prosecution and disciplinary action in the public interest* (May 2019)
- *Improper access to public sector databases, no.2* (May 2019)
- *Improper access to public sector databases* (February 2018).[250]

The CCC has also developed a flowchart (see page 87) to help agencies identify the relevant factors in assessing allegations, and in deciding what further action to take.

The following case studies are examples of matters that could have been referred to the QPS as there was some benefit received by either the employee or another person. The discussion of these case studies is not intended as criticism of the decision made in these cases, as the CCC recognises that a number of factors, not discussed here, may also be relevant in relation to the decision to refer a matter to the QPS.

248 The CCC has functions under s. 34(1) of the CC Act to raise standards of integrity and conduct in agencies and ensure that complaints about corrupt conduct, including misuse of confidential information, are dealt with in an appropriate way.

249 The CCC may monitor matters through a Public Interest Review (PIR), which involves the highest level of monitoring, or a Merit and Compliance Review (MCR), in which case the CCC reviews the matter after it has been finalised by the agency.

250 All three publications can be found at https://www.ccc.qld.gov.au/publications/prevention-focus-case-studies

Case study: Supervisor disclosed colleague's personal information (DTMR)[251]

Facts

A Senior Transport Inspector in a supervisory role was reprimanded for accessing and disclosing a fellow employee's confidential information, namely a licence suspension, contained in the TRAILS database.

Outcome

The offender remained in his supervisory role and received a pay point reduction for 12 months. The matter was not referred to the QPS.

In relation to the first case study, following a discussion about the disciplinary sanction, Mr Magoffin stated that referral to police probably wasn't on his radar at that time[252]. And, during an exchange with the presiding officer, Mr Magoffin acknowledged that DTMR's attitude towards these matters has become more robust and serious, noting that case study 1 was a number of years old.

Case study: Employee provided contact details for member of the public to colleague (DTMR)[253]

Facts

The offending behaviour took place in 2016 and involved a Senior Processing Officer accessing the TRAILS database at the request of a fellow employee (employee A) who had been involved in a road rage incident. The Senior Processing Officer gave employee A contact details for the other driver, which were used by employee A to abuse and threaten the driver on the telephone. The driver involved in the road rage incident made a complaint to the QPS regarding alleged threats made by employee A during the phone call.

Outcome

DTMR did not refer the conduct of the Senior Processing Officer who accessed the database to the QPS. The disciplinary outcome for the Senior Processing Officers was a pay point reduction for 12 months.

The disciplinary outcome for employee A was termination of employment.

In relation to the second case study , Mr Magoffin stated that the fact that there was no personal gain for the subject officer or loss to TMR in the matter were relevant factors in deciding whether the matter should or should not have been referred to the QPS and also in relation to the appropriate disciplinary sanction.[254]

The CCC acknowledges that a wide range of circumstances should be taken into account by decision makers when determining the appropriate sanction to impose on a subject officer, and that many of these may not be known until after the employee has been issued with a show-cause notice. However, the CCC cautions agencies against using these mitigating circumstances as justifications for not referring allegations relating to misuse of confidential information to the QPS for consideration of criminal charges. While these personal factors are relevant to the penalty they should not be regarded as determinative as to whether a referral to the QPS is appropriate.

---

251 Evidence given by Geoffrey Magoffin on 20 November 2019, pp. 26-27 and Exhibit 151.

252 Evidence given by Geoffrey Magoffin on 20 November 2019, p. 27

253 Evidence given by Geoffrey Magoffin on 20 November 2019, pp. 27- 29 and Exhibit 152.

254 Evidence given by Geoffrey Magoffin on 20 November 2019, p. 30

All agencies are on a continuum in relation to their staff's ability to identify and recognise the need to refer allegations of misuse of confidential information to the QPS. The CCC acknowledges Mr Magoffin's evidence that DTMR has matured considerably [since the above case studies] and DTMR now has a policy, consistent with other agencies, of considering criminal action first. [255]

The CCC recommends in Chapter 7 that agencies provide adequate education and training to agency staff to ensure employees understand the meaning of terms provided for in s.408E of the Criminal Code, which is to be reflected in related policies.

The last identified reason for agencies not referring matters to the QPS relates to responses received by agencies from the QPS following a previous referral. The following case studies demonstrate inconsistent decisions reached in response to similar types of corrupt conduct that involved misuse of confidential information.

Case study: Employee disclosed prisoner's information to other prisoners (QCS) (Case study W)

Facts

A QCS Custodial Correctional Officer accessed the records of three prisoners and disclosed them to other prisoners. The misuse of confidential information came to light by way of a complaint to the QCS on 27 September 2017.

Response

On 12 June 2018, following a QPS referral, the offender pleaded guilty to offending under s. 408E of the Criminal Code and was fined $1200. Then, on 14 September 2018, QCS commenced disciplinary action. Two show-cause notices followed on 14 September 2018 and 18 October 2018, and finally a termination letter on 24 April 2019.

Case study: Employee disclosed prisoner's information on social media (QCS) (Case study X)

Facts

The offender had accessed the prisoner's records on 8 November and 10 December 2018 and disclosed information on her social media site. The misuse of confidential information came to light by way of a complaint to QCS on 8 February 2019, following a fellow staff member identifying a photograph of a prisoner on the offender's social media site. The offender had failed to disclose a conflict of interest in being personally acquainted with the prisoner.

Response

A QPS referral was made on 14 February 2019. That same day the QPS advised that it was not in the public interest to proceed with a criminal investigation. [256]

On 3 June 2019 disciplinary proceedings were instigated which, following the offender's contract not being renewed, led to post-separation proceedings.

255 Evidence given by Geoffrey Magoffin on 20 November 2019, pp. 25 and 36

256 Emails between QCS and QPS on 14 February 2019 (Exhibit 91).

From a comparison of the case studies above, it appears the QPS response was different in each case, despite both matters involving the unlawful access and disclosure of prisoner records by QCS employees — one matter was pursued criminally while in the other it was deemed not to be in the public interest to proceed. QCS in each instance promptly referred each matter to the QPS prior to initiating disciplinary proceedings.

A further case study discussed during the hearings with the DoE delegate involved an employee accessing details of a complaint made by her ex-partner in circumstances of an acrimonious separation involving family law proceedings. Significantly, a comment was made in related correspondence between DoE and the CCC, wherein DoE explained via email to the CCC on 4 April 2019 that one of the three considerations for not referring that matter to the QPS was due to:[257]

> *Recent advice from the QPS regarding referrals under s. 408E in which the QPS have advised that it is not in the public interest to investigate or charge in this instance and further that it is more of an internal matter for the department to determine.*

The CCC recommends that the QPS should be providing clear and cogent reasons to agencies when a decision is made not to commence a prosecution, in order to prevent agencies applying a generalised statement from the QPS as a rule of thumb for future matters.

Inconsistent disciplinary outcomes determined by agencies

The purpose of disciplinary proceedings is to protect the public, uphold ethical standards within units of public administration, and to promote and maintain public confidence in the public sector.[258] An inconsistent approach across different agencies can undermine public confidence in agencies that are seen as too lenient or weak in response to misconduct and corruption involving misuse of confidential information. During Operation Impala, it became evident that there were different practices across the subject agencies when dealing with instances of misuse of confidential information by staff. The case studies below illustrate those differences.

Case study: Accessed own and family's record, employment terminated (Mackay HHS)

Facts

A manager accessed the ieMR records of herself, family, other staff and their family over a period of 19 months.

Outcomes[259]:

A formal disciplinary process was commenced to show cause; the subject officer was temporarily transferred and her access to ieMR was removed during the period of investigation. The matter was referred to QPS, and the employee was terminated at the conclusion of the show-cause process.

257 Email from DoE to CCC dated 2 April 2019 (Exhibit 37).

258 CC Act, s. 219A

259 Evidence given by Rod Francisco on 12 November 2019, pp. 22-23

Case study: Accessed own and family's record, reduction in pay point (GCHHS)

Facts

An administrative officer accessed her own and her family's records over the course of one year on 77 occasions on the eMR database. (This case study is described in greater detail in Chapter 5).

Outcomes

The disciplinary sanction was a reduction in pay point and a reprimand,[260] and the matter was not referred to the QPS, despite the CCC recommending to the contrary.[261]

For what were relatively similar matters it can be seen that there were significantly different outcomes for the employees.

Based on information obtained during Operation Impala, Mackay HHS demonstrated a mature approach for dealing with breaches of confidential information, shown by:

- Incorporating a decision-making matrix to assess the seriousness of an employee's conduct
- Evidence obtained during the information-gathering stages of Operation Impala that Mackay had a systematic approach to considering the allegations against a number of relevant factors including:
  - the seriousness of the substantiated allegations
  - the employee's overall work record, including previous disciplinary action
  - any explanation given by the employee, including any extenuating circumstances which may have had a bearing on the employee's actions or the incident
  - the degree of risk to the health and safety of staff and clients
  - the impact the substantiated allegations had had on the employee's ability to perform the duties of their position, and
  - the impact the substantiated allegations has on public and client confidence in Queensland Health and Mackay HHS.

By comparison, GCHHS is not yet as established in terms of its approach and processes in dealing with misuse of confidential information with the ieMR. This is not surprising, given the comparatively shorter time that GCHHS has been working with the new system.[262] Although GCHHS has terminated some employees,[263] there has only been one QPS referral in the four preceding financial years.[264]

Hannah Bloch, Executive Director of People and Corporate Services, detailed the following instances where a QPS referral would be considered:[265]

- malicious intent
- involvement of external people, and
- a repeat offender.

---

260 Evidence given by Hannah Bloch on 13 November 2019, p. 20; Exhibit 58.

261 Letter CCC to GCHHS dated 2 April 2019 (Exhibit 58), p. 3.

262 Mackay HHS was one of the first HHSs to commence ieMR having had it in place for over two years. GCHHS only recently commenced using ieMR in March 2019.

263 Evidence given by Hannah Bloch on 13 November 2019, p. 17.

264 Ibid, pp. 17-18.

265 Ibid, p. 18.

A detailed list of factors taken into consideration by GCHHS and used in the disciplinary process, akin to that employed by Mackay HHS, was not available to Ms Bloch at the time of the hearings.[266]

To assist agencies in improving their decision making about which matters should be referred to the QPS for consideration of criminal action, and assist with parity in relation to disciplinary decision making, the CCC has developed an assessment flowchart (see page 87).

In the event that an agency determines not to refer an allegation of misuse of information to the QPS, best practice also requires that a record be made of the reason(s) why the allegation was not referred. This will ensure agencies are accountable and transparent in their decision making. These types of decisions may be subject to an audit by the CCC.

Pursuit of post-separation disciplinary proceedings

Another important aspect of dealing with allegations of corrupt conduct is ensuring that appropriate disciplinary action is taken against not just current employees, but also employees who may have resigned during the course of a disciplinary investigation. This is important for two reasons: it shows that employees can't just walk away from improper conduct without any consequences, and it can also alert other potential employers to the risks associated with the employee's prior conduct. Post-separation declarations are a finding that the employee engaged in misconduct in their previous role.

While there were variances across the subject agencies about when and to what extent post-separation disciplinary proceedings were pursued, all witnesses questioned as part of Operation Impala attested to the desirability of post-separation disciplinary declarations. There was a general consensus that such declarations function as an invaluable tool in an effective risk mitigation strategy.

The information obtained from some agencies demonstrated a strong stance in pursuing post-separation disciplinary declarations. DoH's number of post-separation declarations was generally low within DoH and the HHSs — for example, three for DoH over the preceding four financial years[267] and one for GCHHS for that same period.[268]

Assistant Commissioner Sharon Cowden, Ethical Standards Command, noted that the QPS Professional Practice Managers (PPMs) advise the decision makers on whether or not post-separation disciplinary action should be taken, and advised that a PPM training course had recently been implemented with a view to building the capacity and capability of the PPMs. This was to ensure that a more robust system to consider post-separation disciplinary action was adopted by the QPS.[269]

The CCC strongly urges all agencies to pursue post-separation disciplinary declarations where they have appropriate grounds and that course is available under the legislation.

One of the benefits derived across the public sector from post-separation disciplinary declarations is to apprise future prospective employers of this information as part of the pre-employment vetting process. To that end, appropriate pre-employment screening and vetting processes are necessary to ensure an agency is privy to the complete background of candidates.[270] Pursuing post-separation disciplinary declarations as a means of officially documenting the wrongdoing of a previous

266 Ibid, p. 19.

267 Part 5 Disciplinary Action, DoH Response for Information from Agencies.

268 Part 5 Disciplinary Action, GCHHS Response for Information from Agencies (Exhibit 57).

269 Evidence given by Assistant Commissioner Cowden on 18 November 2019, p. 8.

270 IBAC (2020), Recruitment and Employment (webpage article, 2020), <https://www.ibac.vic.gov.au/preventing-corruption/are-you-vulnerable-to-corruption/recruitment-and-employment>.

employee may therefore operate as an effective risk mitigation tool when used in conjunction with appropriate vetting procedures by other agencies.

Risks associated with disciplinary processes occurring first in time

Often agencies are in a position to investigate and deal with allegations of misuse of confidential information quickly, and to take action to ensure that the employee who is alleged to have acted inappropriately is prevented from being able to reoffend.[271] Agencies with a mature IT system that enables staff to identify dates and times that employees accessed particular data can readily determine if that access appears lawful or whether it requires further investigation.

The downside of an agency commencing a disciplinary process before reporting the matter to the QPS is that it will almost always involve the agency disclosing to the employee that they are suspected of having engaged in corrupt conduct and/or a criminal offence. This course of action carries risks that it might compromise any subsequent criminal investigation.

These risks can include an employee destroying or concealing evidence of their wrongdoing, and/or approaching other witnesses and coercing or improperly influencing any subsequent statement they may provide to police. There is also the risk that evidence gathered during disciplinary investigations may be tainted if it is not gathered according to accepted standards and practices required for a criminal prosecution. Often employees tasked with collecting evidence for a disciplinary matter do not have the training or experience to ensure that it is gathered to the appropriate standard required to meet the rules of evidence in a criminal trial. This is not intended to be disparaging of public sector employees, it is merely recognising that they do not have the same training and experience as police officers.

Undue delays in reporting a matter to the QPS, pending the outcome of the disciplinary matter, may also result in the QPS being precluded from charging, having regard to the 12-month time limitation imposed by s. 408E(1) of the Criminal Code in situations where no proven detriment has been suffered or no benefit gained.

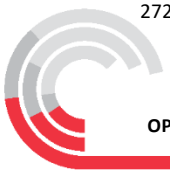
Even where the initial allegations suggest that the employee's conduct is not serious — for example, it may have been a "once off" and did not involve a breach of a third party's privacy — subsequent investigations may reveal that the conduct is more serious and protracted.

Both HHSs acknowledged that QPS referrals were not always made prior to the instigation of any disciplinary process[272]. While this approach reduces the risks to the agency from the employee's conduct, if the agency responds quickly to the incident, it may be cause for concern if evidence is not collected correctly where criminal charges are subsequently referred to the QPS.

Resolving the tension between, on one hand, taking timely disciplinary action to protect the agency and, on the other, ensuring an effective criminal investigation can be conducted, requires two key components: a sound risk assessment by the agency at the outset and prior to any disclosure to the suspected employee that they may be under investigation; and clear directions by the QPS regarding relevant material required to assist it to conduct a timely assessment as to whether a criminal prosecution is possible and warranted.

271 For example an employee could be suspended, transferred to another area of the agency or have their access to the database removed.

272 Evidence given by Rod Francisco on 12 November 2019, p. 23; evidence given by Hannah Bloch on 13 November 2019, p. 25.



The flowchart on page 87 should help agencies assess the risks and determine the seriousness of the misuse of the confidential information. Also, in relation to the role of the QPS in providing timely support to agencies, the CCC has made a recommendation to the QPS designed to assist agencies provide relevant information to the QPS to enable timely and consistent decisions to be made.

Best-practice principles

To address the issues discussed above, the CCC has identified the following best-practice guidelines for agencies to adopt when dealing with allegations of misuse of confidential information.

Pursuit of criminal prosecution in the first instance

The preferred course of action for all agencies is for the agency to consult with the QPS prior to commencing their own disciplinary process. If the QPS considers it appropriate for the agency to commence disciplinary process first, then the agency should do so.

In some cases the criminal investigation and the disciplinary process can be done concurrently. The CCC recommends that the agency liaise with the QPS case officer to ensure the disciplinary process does not interfere with the criminal investigation.

The main risk with the disciplinary process proceeding first is that the agency may not deal with the evidence well and the process may taint it for any future criminal trial. Another risk of delaying the decision to refer matters to the QPS is that the time limitation for charging will have elapsed and the criminal offence may not be able to proceed. For these reasons the CCC recommends that the QPS provide agencies with guidance on what additional information should or can be collected by the agency without compromising the investigation while still ensuring that sufficient time remains to commence a criminal prosecution, if appropriate (discussed further below).

Decision-making framework to be applied to improve consistency

Inconsistent decisions made by agencies when determining disciplinary outcomes contributes to employee confusion and may detrimentally impact on organisational culture in relation to the management of confidential information. Also, different decisions regarding whether particular matters warrant referral to the QPS to consider whether a criminal investigation and/or criminal charges should be commenced can diminish public sector confidence in government's ability to manage confidential information of members of the public.

A further measure to improve clarity and understanding throughout the workplace is to ensure that decision making regarding misuses of confidential information are uniform, transparent and defensible. To that end, the flowchart on page 87 is recommended for use by all public sector agencies when dealing with allegations of misuse of confidential information. This flowchart is a guide only and the individual circumstances of the case might require a more nuanced response. The CCC strongly encourages agencies should tailor this flowchart to suit their particular agency needs and the environment in which they operate.

How to use the flowchart

The flowchart describes some of the key decisions that assessment officers must make when assessing allegations of misuse of confidential information. The flowchart has been designed to guide decision makers to the most appropriate type of action to take in each case, in terms of potential disciplinary and/or referral to the QPS for consideration of criminal charges. Agencies may wish to refine some of the questions in the flowchart to meet their particular needs.

The first decision involves an assessment of whether or not the misuse of information resulted in a breach of a person's privacy. For example, has the officer accessed their own information or the information of a third party with their consent? Accessing confidential information where that does not interfere with another person's privacy may not be as serious as allegations which do. Where the officer has accessed confidential information of another person, not related to their work, that conduct should be considered as serious.

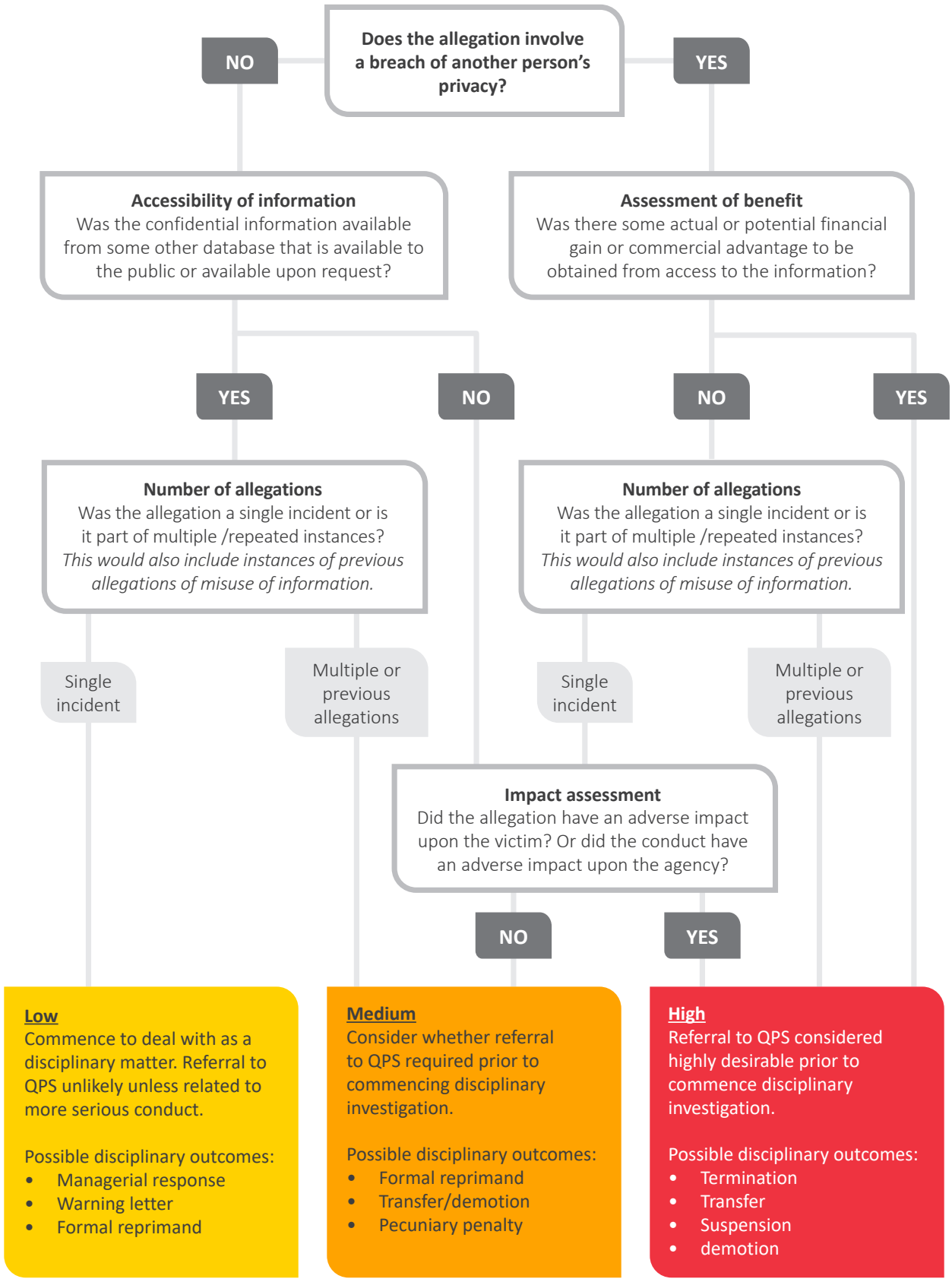
An assessment of whether the information was available from some other source may determine the seriousness of the conduct. For example, the officer could have obtained information which was already available by other lawful means but inappropriately accessed a confidential database because it was "easier" or "more convenient". In this case, a single incident might be appropriately dealt with through managerial action. However, had the officer repeatedly used the database to obtain information that would not otherwise be available, this would have to be considered a more serious breach.

The number of times an officer accesses information inappropriately can be a factor which increases the seriousness of a complaint. This may involve some discretion by the decision maker. For example, if the officer accessed the information multiple times the same day or multiple times over a period of months, this would increase the severity of the matter.

Lastly, one of the considerations for decision makers is the impact of the unauthorised access on both the person whose information was accessed and the agency. A related consideration is whether the information was disseminated to a third party. Assessing the impact when an allegation is first made can be difficult, because once the information is accessed and disseminated it can result in unintended consequences which may not be immediately apparent. For example, an officer who discloses a person's address may be unaware that the person to whom the information is given intends to assault the other person. Nonetheless, the decision maker should consider the potential implications of the improper access or dissemination of the confidential information.

The recommended agency responses contain a range of outcomes intended to reflect the need to be responsive to the particular circumstance of each individual allegation.

Assessing a suspicion of corrupt conduct involving misuse of confidential information



QPS agency support

The current systems employed by the QPS to deal with agency referrals relating to misuse of confidential information fundamentally face three challenging aspects:

- delay
- (an apparent) reluctance to charge based on public interest considerations, and
- inconsistencies in both procedures and outcomes, depending on where the complaint is received within the QPS.

One of the major benefits in consistency with respect to the manner in which the QPS deals with the various complaints received from agencies is improvement in the public's trust and confidence in the agencies, in particular the QPS.

The Commissioner of Police, Katarina Carroll, acknowledged these flaws and the need for change. Last year the QPS identified misuse of confidential information as one of the three serious types of misconduct of its staff warranting specialised management through a central unit to ensure a consistent and effective approach to all such internal cases, as emphasised by Commissioner Carroll:

> *What is incredibly important here is that if such contravention occurs, appropriate and proportionate discipline and criminal action be taken. In that regard, QPS has mandated that all information access or misuse matters* [by police officers] *must be referred to the Office of State Discipline and dealt with at the most senior level within the organisation as a means of providing consistency and determinations in outcome and to reflect the level of importance based on this type of conduct.* [273]

When discussing the current delays experienced by referring agencies in getting a response from the QPS with respect to the position taken on prosecution, and reluctance to prosecute encountered in some instances, Commissioner Carroll explained:

> *I can't offer a reason as to why the delay. And nor can I offer a reason as to why a detective or a police officer mightn't pursue the matter criminally …the Queensland Police Service is getting complaints at a very local level*
>
> *In the past, what used to happen it used to come into the organisation at a very high level and then it would be farmed out to the appropriate levels. So at the moment that is not occurring. So each – there is no consistency as to the way it is being dealt with across the organisation.*
>
> *… you are correct, it needs to be done in a very, very timely manner in order for it to have great effect.* [274]

Commissioner Carroll stated that there was already a QPS committee looking into the potential to again have all misuse of confidential information matters from public sector agencies directed to and dealt with at a "very high level".[275]

Reasons to be provided to agencies

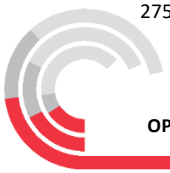
Detailed reasons for pursuing or not pursuing criminal charges should be made available to agencies. This may help bolster sector-wide understanding of considerations taken into account by the QPS when determining whether or not to charge, which may in turn strengthen the referral process.

---

273 Evidence given by Katarina Carroll on 18 November 2019, p. 4.

274 Ibid, pp. 47-48.

275 Evidence given by Katarina Carroll on 18 November 2019, p. 48.



In determining whether or not to charge for all types of criminal offence, police follow the general prosecution policy contained in Chapter 3 of the QPS' *Operational Procedures Manual* (OPM).[276]

There is a two-tiered test:

1. sufficiency of evidence; and
2. public interest.

If there is sufficient evidence, the decision on whether or not to prosecute requires a consideration on whether there is a public interest in pursuing the charge. There are various public interests which must be weighed up in determining if there is an overriding public interest in prosecution on a case-by-case basis.

The QPS has determined that in all civil applications for a Protection Order in domestic violence matters pursuant to s. 37 of the *Domestic and Family Violence Protection Act 2012* (Qld) it is always in the public interest to pursue. This QPS position, in a case of misuse or disclosure of confidential information involving a domestic violence victim, is such that it will always be in the public interest to prosecute under s. 408E of the Criminal Code. The Commissioner of Police, Katarina Carroll, confirmed this sentiment when she stated in evidence: [277]

> *Yes, and that's a strong message that I have sent.*

It is considered that the QPS providing clear and cogent reasons to agencies as to why a particular matter did not result in a criminal prosecution will increase agencies' understanding of which matters are likely to result in a criminal prosecution. Simply stating that the matter is not in the public interest does not provide any guidance to agencies as to why that particular matter was not prosecuted, and could lead to agencies applying this generalised response to other matters concerning a misuse of confidential information.

Complaint template and guidelines

It became evident that the seven agencies varied widely in their respective approaches to dealing with misuse of confidential information by staff, in terms of both disciplinary action and the decision to refer matters to the QPS for consideration of criminal charges.

Moving forward, the CCC considers that overall direction by the QPS to agencies would improve agency-specific practices and procedures, to effect a uniform and consistent approach to the misuse of confidential information across the public sector.

A template and guidelines should be provided to all agencies, comprising:

- Proforma sections to complete for both the initial referral, including information about the type of information accessed, whether it has disclosed to a third party, the number of occasions this occurred and the time period over which it occurred.
- Proforma sections to complete when and if the QPS requires further information. For example, the QPS may require particular information about the database from which the information was obtained, including whether it can obtain a detailed audit and explanation of the IT system, and
- Identification and advice as to factors identified by the QPS of particular relevance to the offence of misuse of confidential information by public officers.

This will enable the QPS to more efficiently identify matters which warrant criminal prosecution, and result in quicker decisions and a consistent and defensible approach to decision making.

276 OPM Ch. 3 (Exhibit 106).

277 Evidence given by Katarina Carroll on 18 November 2019, p. 40.

Recommendation 6 – Dealing with misuse of confidential information

That public sector agencies:

1. Consider criminal prosecution upon detection of misuse of confidential information by public sector employees, which generally will require the matter be referred to the QPS as a criminal complaint in the first instance prior to a determination being made with respect to the instigation of disciplinary proceedings.
2. Apply and adapt, if necessary, the CCC's assessment flowchart to ensure consistency in decision-making processes with respect to incidences of misuse of confidential information, including the decision to refer to the QPS and the decision to institute disciplinary proceedings. Public sector agencies are to retain contemporaneous records to justify decisions made.
3. Pursue post-separation disciplinary proceedings where appropriate.

Recommendation 7 – Referral for criminal proceedings

That the QPS:

1. Manage all complaints of misuse of confidential information by public sector employees through the central QPS unit in the first instance.
2. Provide clear and cogent advice to agencies in relation to the reasons for not commencing criminal prosecutions when matters are referred from the agency.
3. Provide a template and guidelines for public sector agencies to refer a suspected criminal with respect to misuse of confidential information to assist with the compilation of relevant information for the QPS to use during the determination to commence an investigation.

Chapter 9 — Improving prevention and detection systems

Throughout both the investigative and public hearing phases of Operation Impala it became apparent that certain members of the public, by reason of their particular vulnerabilities, should be afforded additional protection from public officers misusing their confidential information.

All expert and agency witnesses agreed that domestic violence victims constituted such a class of person. Certain witnesses identified that another category of people more likely to have their confidential information misused was high-profile persons, including sports personalities, politicians and members of the public who suddenly become the subject of media attention due to some event or incident.

The additional protections for vulnerable persons should include both improved prevention and detection systems.

Domestic violence victims

This category of person is easily identifiable, as the person identifies themselves as a victim of domestic violence to the agency. Some agencies (such as the QPS and QCS) could also proactively identify these parties by reason of them being an aggrieved person named on a Protection Order made pursuant to the *Domestic and Family Violence Protection Act 2012*.

Professor Barbara McDonald considered that a serious invasion of privacy would occur if a domestic violence victim, who was concealing their address from an ex-partner, had their contact information disclosed.[278] In her view, the level of protection of a person's privacy is dependent upon the level of risk following a breach:[279]

> *One of the problems with privacy is that it is not an absolute value or an absolute freedom … privacy is very much a relative matter.*
>
> *But you asked about victims of domestic violence. We had a lot of submissions [for the ALRC 2014 Inquiry] from various entities and groups about the way in which electronic intrusions and electronic collection of information, misuse of information, disclosure of information, was often a precursor to domestic violence. … So, undoubtedly, everybody's entitled, no matter who they are, to protection of their privacy. And obviously the more so when there is a risk to their life and health and safety.*

Professor McDonald opined that in relation to more sensitive information, including that of a domestic violence victim:

> *I certainly think that [there] would have to be a regular audit.*[280]

Sarala Fitzgerald was firm in her view that vulnerable persons, including domestic violence victims, should be afforded additional protections.[281]

278 Evidence given by Professor Barbara McDonald on 15 November 2019, p. 14.

279 Ibid, p. 15.

280 Ibid, p. 22.

281 Evidence given by Sarala Fitzgerald on 19 November 2019, p. 14.

"Privacy by Design" (PbD) (discussed in Chapter 12) requires agencies to take more stringent steps to prevent the misuse of confidential information in circumstances where there exists a likelihood of harm occurring from its disclosure, which includes physical harm in circumstances where a domestic violence victim's address has been disclosed to her ex-partner.[282]

High-profile persons

Agencies may need to develop a proactive approach to identifying members of the public whose confidential information they hold, and could be at risk of being accessed or misused because of their profession, position or media interest.

The CCC has identified that additional protection should be afforded to this category of person, due to the increased risk of their records being accessed by employees. Rod Francisco from Mackay HHS gave evidence of excessive searches being undertaken on the records of high-profile patients.[283] Further, Mr Francisco explained that high-profile persons included otherwise ordinary members of the public who attracted media attention as a result of an incident, citing the example of two Englishmen in the Whitsundays involved in a shark attack.[284] The Queensland Information and Privacy Commissioners are of the opinion that "high-profile individuals may also be at greater risk of having their personal information accessed unlawfully". Their submission at (paragraph 3) provides two examples from DoH and the QPS.[285]

Each agency should identify its own categories of vulnerable persons, including, as a minimum, domestic violence victims and high-profile persons.

Agencies' current functioning and capabilities

In this section, the current functioning of each agency's systems and processes will be examined, in order of appearance at the public hearings, to determine whether the system is being utilised to its full capability with respect to affording vulnerable persons additional protection from misuse of their confidential information. Evidence was given by some agencies of advanced systems, including the deployment of data analytics. This evidence will be summarised for the benefit of other agencies.

It is acknowledged that improvements to systems are dependent upon sufficient financial and staff resources. However, PbD makes it clear that:[286]

> *The practicality of implementing a security measure, including the time and cost involved, will influence the reasonableness of taking that step.*
>
> *However, you are not excused from taking specific steps to protect information just because it would be inconvenient, time-consuming or costly to do so.*

Relevant factors in this assessment process include the size of the agency and the sensitivity of the information stored on their systems.[287] All seven agencies are large entities relative to others subject to the requirement to comply with PbD, and they all hold sensitive information on behalf of the public such as contact and financial details, criminal and health records. Consequently, there is a

282 Ibid, p. 14.

283 Evidence given by Rod Francisco on 12 November 2019, pp. 10 & 25.

284 Ibid, p. 20.

285 OIC submission received on 9 October 2019, p. 1.

286 OAIC (2018). *Guide to securing personal information: "Reasonable steps" to protect information*, p. 15.

287 Ibid 13.

requirement for all of these agencies to take more stringent steps than other smaller entities holding less sensitive information.

It is of concern to the CCC that two of the agencies professed to follow the PbD approach (DoH[288] and the QPS),[289] yet both agencies had great deficiencies. DoH has capacity to improve as system manager[290] over the HHSs to ensure consistency amongst the HHSs: GCHHS does not undertake any manual auditing, whereas Mackay HHS does; and GCHHS does not place flags on records of domestic violence persons, whereas Mackay HHS does. The CCC notes that while DoH is aware of the benefits of PbD and is promoting these practices, there is scope to further mature its application of these principles. The QPS has a fully auditable system that is not proactively audited; the system is able to add flags to identify domestic violence victims but this is not used as a prevention method to protect their privacy. (See below for a discussion of flags and how they can assist with privacy.)

The main databases used to hold the public's confidential information were focused on during the public hearings, as detailed below; however, the recommendations contained in this report are directed to all databases holding the public's confidential information, including contact details.

QCS

The Integrated Offender Management System (IOMS) is the main database holding personal information. The database holds a range of personal information not only of prisoners, including health details, but also of their visitors, in addition to a victims' register.[291]

Although the database logs all accesses and is auditable, proactive manual audits are generally not undertaken.[292] There are weekly audits of particularly vulnerable persons, namely a weekly audit of the victims' register, and yearly audits of the entire IOMS system of the access logs. However, the QCS is currently working on improvement in this area, as detailed below.

IOMS is a dated system.[293] Even so, flags are able to be placed on records of vulnerable and high-profile prisoners. Access to flagged records generates an automatic report which is sent to a senior officer.[294] It was not apparent, however, that these flags were being used to the extent required to afford the necessary additional protection to vulnerable and high-profile prisoners.

Since becoming a separate entity in 2017 (it was previously part of DJAG), QCS's ability to excel in this area has been constrained by lack of sufficient resources. Following the release of the Taskforce Flaxton report in 2018, the Government, as part of the State Budget released in July 2019, allocated $2.5 million to QCS to undertake the immediate remediation work recommended in the report.[295] Recommendation 27 included the replacement of IOMS, which is "inevitable"[296] but:

> *to replace a system as complex as IOMS would be a very laborious time consuming complex endeavour and costly … and require an investment from government.*[297]

The remediation work comprises two elements. Firstly, the enhancement of the IT services within QCS. A comprehensive review was undertaken, followed by the current recruitment of additional

288 DoH response to CCC questions, p. 24 (Exhibit 68).

289 QPS response to CCC Request for Information from Agencies (Exhibit 98).

290 HHB Act, s. 8(3).

291 Evidence given by Dr Peter Martin on 11 November 2019, p. 12.

292 Evidence given by James Koulouris on 15 November 2019, p. 11.

293 Evidence given by Dr Peter Martin on 11 November 2019, p. 25.

294 Evidence given by Dr Peter Martin on 11 November 2019, p. 25.

295 Evidence given by James Koulouris on 15 November 2019, p. 10.

296 Evidence given by Dr Peter Martin on 11 November 2019, p. 14.

297 Ibid, p. 19.

staff for the IT area. Secondly, QCS has engaged a project manager, business analysts and programmers to deliver enhanced information security.[298]

> *The key focus of that work initially will be on a more proactive stance in being able to identify the inappropriate use of the IOMS system from both an auditing and a deterrence and a prevention aspect. So there's a number of elements to that that we're actively looking at. One is to enhance the ability to undertake proactive audits of usage of IOMS.*[299]

Another avenue QCS is exploring is development of the ability to identify unusual activity within IOMS, for example where a record is accessed by multiple people at multiple locations concurrently.[300]

Furthermore, in response to Taskforce Flaxton's Recommendation 8, which includes the development of strategies to address capability gaps in IT, QCS commissioned an independent consultancy company to look into its IT vulnerabilities.[301]

QCS Commissioner, Dr Peter Martin, emphasised the impact that Taskforce Flaxton had on the functioning of QCS:[302]

> *Evidence that I gave at Taskforce Flaxton hearings allowed me to articulate my vision for the future of Queensland Corrective Services. Guided by the now released Corrections 2030, a blueprint for the future of our organisation, we're shaping Queensland Corrective Services into a future-focused innovative and professional top-tier public safety agency.*

Guided by this 10-year strategic plan, and committed to organisational reform and transformative change, the organisation is changing and evolving. QCS is to be commended on its efforts thus far to implement all of the 33 recommendations of Taskforce Flaxton:[303]

> *Through Taskforce Flaxton, we identified, with the assistance of the Crime and Corruption Commission, a number of key improvements to Queensland Corrective Services' operation as we build our capability. And I'm very pleased to say, with assistance of Government, we're well on our way in delivering that, and making our commitment to make good the 33 recommendations of that important report.*

DTMR

DTMR has the most advanced and effectively run system out of the seven subject agencies. It is a mature system. Operation Impala examined DTMR's TRAILS/TICA database.

Both databases log all accesses. DTMR employs an extensive regime of data analytics. There are several analytics and scripting processes, which take place overnight, checking for unusual access, including out-of-hours and excess access. Reports on unusual access are produced instantaneously and referred to the compliance area in the Customer Services and Safety Regulation division, where

298 Evidence given by James Koulouris on 15 November 2019, pp 10-11.

299 Ibid, pp 10-11.

300 Ibid, p 11.

301 Evidence given by Dr Peter Martin on 11 November 2019, p 14.

302 Ibid, p 10.

303 Ibid, p 11.

action can be taken within one day's notice.[304] There is also an Information Security Unit which is able to work directly into the Ethical Standards Unit.[305]

Two examples of speedy proactive detection of privacy breaches, both detected the next business day, were discussed during the evidence of Sandra Slater, Chief Information Officer. The first breach (an email sent, attaching a demerit history for the employee's son) was detected as a result of monitoring of outbound emails; the second (use of a member of the public's details to falsify an 18-plus card for the employee's partner) was detected through identification of a photograph mismatch by the Identity Management Unit.[306]

The internal audit reports to the Audit and Risk Committee, comprised of external members as a check and balance.[307]

DTMR's Director-General, Neil Scales, has a particular interest in protecting victims of domestic violence, which is reflected in the protections DTMR provides to this category of vulnerable person:[308]

> *Well I'm a champion against domestic violence. …We have a system in place which is called a Customer Records Suppression Service. If a victim of domestic violence has a court order, we can suppress the information … so that only a small unit within the customer service branch can see that data. … [In addition, whenever the record is accessed] it sets a flag off, and we'll investigate that. It is self-policing.*

DoE

The OneSchool database holds a range of sensitive personal information, including around the medical, behavioural, financial and legal matters of students and staff.[309] OneSchool logs all accesses and is fully auditable.

Even though information management and the security of confidential information is one of four identified risks detailed in the DoE's Enterprise Risk Management Framework,[310] it was not apparent from the evidence given by Director-General Tony Cook whether DoE conducts any form of proactive auditing of access to OneSchool. This is despite DoE having an established Audit and Risk committee.[311] From Mr Cook's evidence it appears that the privacy-specific internal audit regime is confined to access controls, and use of the cloud.[312] However, DoE checks for unusual activity by employees in the system.[313] The OneSchool database is limited in terms of its ability to add flags to the records of vulnerable persons.[314]

DoH, Mackay HHS and GCHHS

DoH owns and controls the databases used by the HHSs. Damian Green, Chief Executive Officer, eHealth Queensland, explained that eHealth Queensland provides enterprise ICT services to the Queensland Health system, including DoH and HHSs. The Integrated Electronic Medical Record

304 Evidence given by Sandra Slater on 11 November 2019, p 5.

305 Ibid, p 9.

306 Ibid, pp 8-9.

307 Evidence given by Neil Scales on 11 November 2019, pp 7-8.

308 Ibid, pp 12-13.

309 Evidence given by Tony Cook on 12 November 2019, p 5.

310 DoE Enterprise Risk Management Framework (Exhibit 28).

311 Evidence given by Tony Cook on 12 November 2019, p 35.

312 Ibid, p 12.

313 Ibid, pp 27-28.

314 Ibid.

(ieMR) is the key clinical information system, which has been deployed in 14 of the 16 HHSs over the last couple of years. eMR is the predecessor to ieMR. Both systems are fully auditable. [315]

The P2Sentinel software is a proactive auditing tool, managed by eHealth. It is able to audit both databases and generate reports, which are assessed by the individual HHSs.

The Hibiscus database is able to have flags attached to vulnerable persons' records; however, currently the flag is only able to warn the user and is not able to send an automated notification to another employee.[316]

The HHSs have encountered problems with the P2Sentinel software which has caused problems with the roll-out of the ieMR database. The P2Sentinel started to be deployed around the time of this roll-out, hence the eMR database has not experienced similar difficulties with backlogs. The reports generated by P2Sentinel of potential breaches (misuse of information by staff) are voluminous and time-consuming to action, which has resulted in backlogs in both subject HHSs. Mackay HHS has had the ieMR database for longer than GCHHS and over that time has matured in its approach to both the database and the P2Sentinel reports. Dr John Wakefield, Director-General of DoH, acknowledged that lessons learnt in Mackay may assist with dealing with backlogs in other HHSs.[317]

One protective action undertaken in Mackay is the triaging of potential breaches by using a "severity matrix", where domestic violence victims are prioritised.[318] Another is the addition of both domestic violence victims and high-profile persons to the ieMR VIP category of record, where a warning flashes up on the screen to alert the user that unauthorised access is prohibited.[319] GCHHS does not use either of these forms of additional protections for domestic violence victims, but adds high-profile persons to its VIP category.[320]

Currently, the automated audits are set up only for "same name" searches. However, Mr Green gave evidence that the functionality capability of P2Sentinel is far greater, which could include additional protection for vulnerable persons:[321]

> *There are a number of mechanisms by which you can audit within ieMR. … There are other types of searches [apart from record of a similar name] that you can do using that functionality, such as if you have a particular interest around who's been accessing a particular patient record … There are about 10 different types of searches … a specialist report [can be logged]…*

DoH has set in place the mechanism to mature this auditing tool. A health information management working group, with its terms of reference as P2Sentinel, has been established. One focus is to develop a list of potential scenarios to audit, and determine how P2Sentinel can be further configured to provide that information. Another focus is maturing the current reports by way of more proactive analytics to generate more specific and shorter reports.

At present GCHHS is receiving these reports on a weekly basis and actioning those reports within three to five days, which is preferable to monthly reporting.[322]

---

315 Evidence given by Damian Green on 14 November 2019, p 4.

316 Evidence given by Dr John Wakefield on 14 November 2019, p 16.

317 Ibid, p 27.

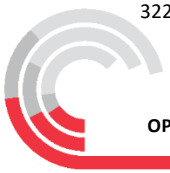
318 Evidence given by Rod Francisco on 12 November 2019, p 12; IeMR Inappropriate Access – Severity and Actions Guide (Exhibit 48).

319 Evidence given by Rod Francisco on 12 November 29019, p 20.

320 Evidence given by Hannah Bloch on 13 November 2019, p 16.

321 Evidence given by Damian Green on 14 November 2019, p 7.

322 Evidence given by Hannah Bloch on 13 November 2019, pp 12-13.



Dr Wakefield warned about the negative consequences of adding too many flags:[323]

> *What I'm asking my team is, if that is a particular issue for us as a flag that has a high yield for potentially inappropriate access, let's get that upfront in the system, that's what contemporary safety systems design does. It doesn't wait and create a retrospective industry which has a whole lot of noise behind it. … Our objective is to minimise inappropriate access. That's a very important way of doing it, which is what we would call low effort, but high impact.*

Dr Wakefield expanded on this concept by explaining his future plan to obtain a new program to enable use of artificial intelligence to build in learning patterns which are much more sophisticated than that which will provide a much higher yield.[324]

Mr Green, newly appointed to his current position, shared his positive vision for the future:[325]

> *My key vision, or one of the reasons I wanted this role, is to help ensure that eHealth Queensland is applying more of a role in supporting our Hospital and Health Services invest in those innovative-type works but also share and collaborate across the health system.*

The current automated audit reports only cover "same name" searches. Manual auditing for other searches is left up to the individual HHSs to manage. Across the two subject HHSs there are significant differences in practices. Mackay HHS has a manual audit plan, whereas GCHHS does not undertake any such audits.[326] Dr Wakefield considered that manual auditing is necessary.[327]

Of particular concern to the CCC is the outstanding backlog of potential breaches of privacy on the ieMR database. Although Dr Wakefield undertook to look into addressing these inconsistencies, and in particular the backlogs,[328] the CCC considers that the backlog of potential privacy breaches presents a significant risk to the public and warrants a separate recommendation in this report.

The evidence from the two subject HHSs indicates a serious backlog in each agency, which is being handled differently by each agency.

Rod Francisco, the Executive Director of People, Mackay HHS gave evidence that the current backlog is about 1000 flagged reports dating back to 2018.[329] Mr Francisco explained that Mackay HHS has developed a severity matrix for triaging the potential breaches.[330] The matrix is used for new breaches, whereby matters involving a risk of harm are prioritised almost immediately and the backlog is dealt with on a capacity basis, without any assistance from DoH.[331] Mr Francisco estimated that Mackay HHS would remove its current backlog if DoH provided one dedicated employee for 12 months, noting:[332]

> *We believe that would be highly efficient because the person who was doing this would start to see patterns and be able to take very similar approaches to a number of the breaches.*

---

323 Evidence given by Dr John Wakefield on 14 November 2019, p 24.

324 Ibid, p 25.

325 Evidence given by Damian Green on 14 November 2019, p 10.

326 Evidence given by Hannah Bloch on 13 November 2019, pp 16-17; Evidence given by Rod Francisco on 12 November 2019, p 17.

327 Evidence given by Dr John Wakefield on 14 November 2019, p 33.

328 Evidence given by Dr John Wakefield on 14 November 2019, p27.

329 Evidence given by Rod Francisco on 12 November 2019, p 12.

330 Evidence given by Rod Francisco on 12 November 2019, p 12; ieMR Inappropriate Access – Severity and Actions Guide (Exhibit 48).

331 Evidence given by Rod Francisco on 12 November 2019, p 15.

332 Ibid p 16.

Even though GCHHS has had ieMR for only a few months, the breaches have mounted up and, combined with the other outstanding potential breaches from the pre-existing eMR database dating back over three years, equate to a huge number — approximately 2500, as shown below (tendered during the public hearings as exhibit 56).

INFORMATION PRIVACY BREACHES FOR GCHHS

Financial Year	**2015-16**	**2016-17**	**2017-18**	**2018-19**
Number of staff involved in privacy breaches.	6	118	713	512
Number of Identified Br. Privacy allegations	8 (No P2 Sentinel reporting for this period)	198 (eMR data base only)	1655 (eMR data base only)	877 (Both eMR & ieMR data bases)
Substantiated breaches	6	10	20	18
Allegations awaiting assessment or investigation	Nil	188	1635	859
Total staff No:	8,671.67	8,965.30	9,502.37	10,059.92
Staff non-compliance rate %	0.069%	1.3%	7.5%	5.08%

Accordingly the CCC has recommended that DoH engage with the HHSs to assist with the resolution of the backlogs.

QPS

A review of the QPS systems and processes for auditing identified a lack of systems and processes to identify and provide additional protections for vulnerable persons. It was also identified that the QPS does not undertake any form of proactive auditing of QPRIME.

The CCC considers that it is particularly concerning that for almost 20 years the QPS has not actioned the recommendation made by its predecessor, the Queensland Criminal Justice Commission, in its report of November 2000 entitled *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*. Recommendation 6.10 of that report provided:

> ***Recommendation 6.10 – Systematic and Ongoing Internal Audit***
>
> ***6.10.1*** *That the Queensland Police Service give higher priority to the use of audit strategies to prevent this type of misconduct by developing and implementing a systematic and ongoing internal audit program, which is both random and targeted, of access to and use of the computer corporate/mainframe systems.*
>
> ***6.10.2*** *That, as part of the risk-management process, managers and supervisors incorporate a program of local internal audit of access and use of computer corporate/mainframe systems*[333]

The Commissioner of Police confirmed that she was aware of this report,[334] and she agreed that currently there is prevalent misuse of information amongst staff in the QPS, noting that currently one in 75 members of the QPS misuse personal information on the QPRIME database.[335]

333 Exhibit 115.

334 Evidence given by Katarina Carroll on 18 November 2019, p 61.

335 Ibid, p 9.

"Niche" is a system at the heart of QPRIME that provides mechanisms to allow for interfaces and integration. The Niche system is used around the world and is produced by a Canadian information technology provider who specialises in policing systems. There exists the ability to access a wider range of tools than is currently accessed by the QPS. There is potential to improve the Niche system to make it easier and cheaper to maintain a future audit trail. Despite all accesses to QPRIME being logged and the system being fully auditable, the QPS does not undertake any proactive auditing except in very limited circumstances, generally linked with operational security issues, rather than having a focus on protecting privacy, without the advantage of a complaint being made.[336] It is acknowledged that once in receipt of a complaint about alleged misuse of QPRIME by an officer the QPS can and does respond by auditing that officer's access to QPRIME. However, in the absence of a complaint, minimal proactive auditing is undertaken by the QPS.

Timothy Dillon, Acting Director of Digital Transformation within PSBA, gave evidence at the public hearings. PSBA provides IT services to the QPS. Mr Dillon spoke about the potential future of the QPS with respect to the use of predictive analysis using data analytics, which would not cost a significant amount but would be time-consuming for the QPS to specify the details of the automated audits that they desire.[337]

Chief Superintendent Matthew Vanderbyl, who leads the Business Improvement Group of the Organisational Capability Command, highlighted the difficulties of the QPS starting any form of manual auditing with the current system:[338]

> *Manual auditing really would be almost impossible to undertake, even on a single digit percentage sampling given the sheer volume of queries that are put in [to QPRIME].*

When questioned further in relation to the QPS' ability to conduct manual auditing of QPRIME, specifically on a selected small group such as vulnerable persons, he accepted that he was sure it could on a sampling basis, but flagged that, given the sheer volume of transactions in QPRIME, the use of data analytics would be more feasible. [339]

Commissioner Carroll was firm in her view that the QPS "should always be auditing", including a targeted audit on the records of domestic violence victims.[340]

Mr Dillon confirmed that the current capability of QPRIME includes the ability to put a flag on a record of a vulnerable person, which generates an automated notification when that record is accessed. The notification can be sent either to a nominated person or role to investigate.[341] Chief Superintendent Vanderbyl confirmed that "you can put a flag on anything, to be quite frank".*[342]*

Commissioner Carroll expressed a reluctance to utilise flags for domestic violence victims:[343]

> *Yes, so flagging vulnerable people. We have got to be very, very careful about this because it is very difficult to make an assessment on the situation if you don't have all of the information. …someone might be an aggrieved tonight, but tomorrow they might be the respondent …*

---

336 Evidence given by Timothy Dillon on 19 November 2019, p 5.

337 Ibid, pp 6-7.

338 Evidence given by Matthew Vanderbyl on 20 November 2019, p 9.

339 Ibid, p 10.

340 Evidence given by Katarina Carroll on 18 November 2019, pp 23 & 27-28.

341 Evidence given by Timothy Dillon on 19 November 2019, p. 11,

342 Evidence given by Matthew Vanderbyl on 20 November 2019, p. 8.

343 Evidence given by Katarina Carroll on 18 November 2019, p. 16.

However, later on in her evidence the Commissioner confirmed that domestic violence victims with domestic violence orders are identifiable in QPRIME and are a category of the public who are at greater risk from privacy breaches involving disclosure, which necessarily means that additional measures to protect them should be put in place.[344]

Best practice

Flags

Agencies involved in Operation Impala gave evidence in relation to their systems' abilities to use flags. Agencies' systems capability varied and included the following capabilities:

- An automated message received by the public officer who accesses the record. In effect, this is a warning to the officer, before accessing the record, that this was a sensitive record that they were about to access, or
- A message sent to a supervisor regarding an employee's access to a particular record, to assess and review.

Both types of flags afford vulnerable persons additional protection from public officers misusing their personal information.

The CCC considers that agencies should utilise their system's capability to the fullest extent possible, with respect to the deployment of flags on records of vulnerable persons to deter misuse of their personal information.

Audits

The deterrent value of audits cannot be underestimated. The mere fact that an agency is conducting audits, and making that known to their officers, provides sufficient incentive not to misuse information on account of the chances of getting caught.

Professor Geraldine Mackenzie emphasized that "the most critical thing is detection" when discussing the purposes for sentencing as set out at section 9(1) of the *Penalties and Sentences Act 1992* (Qld) and in particular:[345]

> *to deter the offender or other persons from committing the same or a similar offence.*

Audits are an "absolutely critical" step for every agency,[346] in complying with its obligations under the IP Act to prevent misuse of the public's confidential information by its officers.

Professor Barbara McDonald was of the opinion that if an agency had a fully auditable system and yet failed to conduct audits, that constituted a failure to take reasonable steps to keep the public's private information contained on its databases secure.[347]

It is the view of the CCC that whilst audits of the records of vulnerable persons are imperative, agencies should also audit their entire systems.

344 Ibid, pp. 20-21.

345 Evidence given by Professor Geraldine Mackenzie on 22 November 2019, p. 8; *Penalties and Sentences Act 1992* (Qld), s. 9(1)(c).

346 Evidence given by Philip Green on 22 November 2019, p16.

347 Evidence given by Professor Barbara McDonald on 15 November 2019, p 21.

Whilst the CCC is cognisant of the need to balance the fiscal and employee resource capacity with the need for audits, the conclusion made following Operation Impala is that each agency must conduct regular audits (at minimum every three months) of at least part of its databases containing the public's confidential information.

The most effective way, from a deterrence aspect, is for each agency to conduct targeted audits. Each agency is to determine, in accordance with the devolution of responsibility, its own category of record to target. This category should comprise the records most likely to be misused by its officers. It became apparent, for example, during the course of the public hearings that this category should include family and friends of staff of QCS, given that four of the five case studies reviewed involved the offender accessing records of their family and/or friends.[348]

Sarala Fitzgerald gave evidence in relation to the Victorian report by the Auditor-General wherein public sector agencies were found to have such significant deficiencies in best practice with respect to protecting the public's confidential information that the report precipitated an amendment to Victoria's privacy legislation. One of the report's recommendations was regular monitoring of access logs.[349]

Until all agencies are in a position of having mature databases where data analytics are deployed, targeted audits should be conducted to provide a minimum level of protection for the public from having their confidential information misused by public officers.

Mature systems

The subject agencies' system capabilities differed greatly, as discussed above. The more mature systems are capable of monitoring outbound emails, after-hours and remote access.

The deployment of data analytics to report unusual access is the optimum process for preventing misuse of information.

Senior Sergeant Matthew Bell from the Victorian Police Service (VicPol) gave evidence during the public hearings. He is the Protective Security Operations Manager of the Security Incident Registry. The function of the Registry is "to record, isolate, contain and consider remediation for protective security events and incidents in Victoria Police".[350]

VicPol is in the process of finding an IT solution for a machine learning system to enable proactive monitoring. Currently, a manual process of proactive monitoring is undertaken, based on cases of vulnerabilities and opportunities that have been exploited.[351] Analysts detect exceptions that are produced by the software, namely potential breaches.

This process is akin to the P2Sentinel monitoring system for the ieMR database utilised by the HHSs. However, VicPol has been using this system for almost two years and effected ameliorations to it over that period, including the generation of fewer and more accurate exceptions, which results in fewer reports to assess. The exceptions are wide ranging, including classified information being externally emailed, irregular volumes of printing, and irregular (by reason of, for example, large volume or lack of business reasons) searches. The exceptions are assessed and then any found to be privacy breaches are triaged and referred either to the local manager or to the Professional Standards Command for investigation.[352]

---

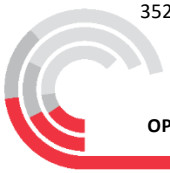
348 Exhibits 85, 88, 89 and 90.

349 Evidence given by Sarala Fitzgerald on 19 November 2019, pp 8-10; Victorian Auditor-General, *Audit Summary of Maintaining the Integrity and Confidentiality of Personal Information*, 25 November 2009 (Exhibit 127).

350 Evidence given by Matthew Bell on 15 November 2019, p 3.

351 Ibid.

352 Ibid, pp 4-6.



The more mature the system, the greater its deterrent and preventative functions in relation to misuse of confidential information. The CCC considers that agencies should look to improving their current systems and obtaining new improved systems to the extent possible, taking into consideration budgetary and staffing constraints.

The QGCIO is well placed to provide advice to agencies with respect to improved proactive auditing systems:[353]

> *We [QGCIO] are set up to provide advice to Government agencies and Executive Government on issues such as setting ICT strategy policies and standards; adopting better practice for ICT investment management; identifying and managing risks including the over-horizon risks; developing a proposal for major whole of government investments and agency investments; improving contract outcomes; and facilitating strategic relationships with industry partners.*

Recommendation 8 – Improved prevention and detection systems

That public sector agencies are to:

1. Develop and define additional protections to safeguard confidential information that relates to vulnerable, including high-profile, persons. Public sector agencies should develop their own categories of vulnerable persons. Protections should be proportional to ensure that operational efficiency is not compromised and should include:
   - flags when records of vulnerable or high-profile persons have been accessed, and
   - targeted quarterly audits of the flags.
2. Conduct quarterly targeted audits of access logs to identify possible misuses of confidential information. Agencies are to develop their own categories for the targeted audits, based on a risk assessment.
3. Develop systems that monitor outbound emails, after-hours and remote access; as well as the deployment of data analytics to report unusual access. That the Queensland Government Chief Information Officer (QGCIO) advise agencies with respect to proposed improved proactive auditing systems.

Recommendation 9 – QHealth

That the Department of Health provide assistance to all Hospital and Health Services to remove the backlogs of potential breaches of the eMR and ieMR databases detected by the P2Sentinel software.

353 Evidence given by Andrew Mills on 20 November 2019, p 5.

Part 4 – Legislative reforms

Operation Impala identified several shortcomings in the legislation used to prosecute public sector employees in relation to improper access to or misuse of confidential information, and in the remedies available to people who have had their information accessed.

Accordingly, Chapter 10 discusses a recommendation to introduce a new offence in the Criminal Code specifically to deal with misuse of confidential information.

Chapter 11 looks at possible amendments to Queensland's privacy legislation and related public sector practices that would improve the protections and remedies available to people who have had their confidential information unlawfully accessed and or disclosed by public sector employees.

Chapter 12 provides agencies with a guide on how to imbed privacy into their day-to-day operations.

Chapter 10 — New criminal offence to deal with misuse of confidential information

Operation Impala identified shortcomings in the legislation dealing with both the sanctions for improper access to or misuse of confidential information, and the forms of reparation available to the affected parties, either from the agency or the public officer involved in the improper conduct.

This chapter examines the relevant current legislation, and why it requires amendment to deal specifically with misuse of confidential information by public sector employees.

Current offence - Computer hacking and misuse (s. 408E)

The offence most often used to deal with public sector employees who improperly access or disclose confidential information is "Computer hacking and misuse" (s. 408E of the Criminal Code).

408E Computer hacking and misuse

(1) A person who uses a restricted computer without the consent of the computer's controller commits an offence.

(2) Penalty—Maximum penalty—2 years imprisonment.

(3) If the person causes or intends to cause detriment or damage, or gains or intends to gain a benefit, the person commits a crime and is liable to imprisonment for 5 years.

(4) If the person causes a detriment or damage or obtains a benefit for any person to the value of more than $5,000, or intends to commit an indictable offence, the person commits a crime and is liable to imprisonment for 10 years.

(5) It is a defence to a charge under this section to prove that the use of the restricted computer was authorised, justified or excused by law.

The intent of the legislators when this offence was drafted was to provide for an offence to prosecute for computer hacking, namely to deal with the (then) growing modern crime involving an external threat of computer hacking and the introduction of viruses.[354]

Professor Geraldine Mackenzie, sentencing expert, explained how the current provision was originally intended to capture hacking behaviour:[355]

> *So at the time that it was introduced which was fairly early on in the days comparatively of using computers, it was about the concept of going into a computer system and introducing harm by viruses or hacking, again, the introduction of harm.*

Employees of public agencies who unlawfully access confidential information may be charged criminally with one of the offences contained in s. 408E of the Criminal Code. Usually, either subsection (1) or (2) is used, depending on the particular circumstances of the conduct.

Subsection (1) is a simple offence, which requires that a charge under this part be commenced within 12 months from the date of the offending, and in limited circumstances, two years.[356] Subsection (2) has no statutory time limit by which to commence a criminal charge, however it requires proof that the subject officer misused confidential information with the intent of obtaining a benefit (discussed

354 Queensland, Criminal Code Advisory Working Group, Report of the Criminal Code Advisory Working Group to the Attorney-General (1996) 75.

355 Evidence given by Professor Geraldine Mackenzie on 22 November 2019, pp. 4-5.

356 S. 52(1) & (2) of the *Justices Act 1886* (Qld).

further below) or to cause a detriment. Subsection (2) attracts a greater maximum penalty and is an indictable offence.

In discussing the problems encountered in prosecuting under the provision, Professor Mackenzie noted:[357]

> *… it* [s. 408E] *doesn't have direct application in these cases, it has been retrofitted, if you like, but has been able to be successful in some cases.*

During the public hearings, Ian Leavers, QPUE, also raised the concern that s. 408E of the Criminal Code was not originally designed for prosecutions for misuse of confidential information by public sector employees:[358]

> *… I do not believe that 408 was created for that. And I go back to the readings in the Parliamentary notes …that were accompanying that and it was designed for those hacking into a system not those who are authorised to* [use] *a system. …*

Challenges in applying s. 408E when prosecuting public sector employees

Accepting that the original intent of the current s. 408E was not to prosecute an employee within a public sector agency for inappropriately accessing or generally misusing confidential information, the current wording of the offence has led to some difficulties in prosecuting employees who have improperly accessed confidential information, as follows.

- The title of the section does not make it clear to public officers that their conduct in accessing confidential information to which they have access in the performance of their duties can be a criminal offence if they do so for an improper purpose. Similarly, evidence given during Operation Impala showed that employees who had password access to confidential information failed to understand that use of that password to access the information could still be a criminal offence under s. 408E.
- The definition of the word "benefit" has led to various judicial interpretations, including that gaining only knowledge from accessing the confidential information is not a benefit.
- The current maximum penalties do not, in the CCC's view, adequately reflect the serious nature of deliberate breaches of the public's privacy by public officers.
- Section 408E does not address the circumstance where an employee accesses confidential information that is not stored on a secure (restricted) database.
- In some cases, charging under the offence becomes statute barred. Examination of the manner in which the subject agencies dealt with instances of staff misusing information has led the CCC to conclude that there are delays, often lengthy, in agencies taking action, and further delay when the matter is referred to the QPS. Moreover, the QPS may hold off on charging if there is a concurrent investigation in relation to the public officer for a more serious offence, noting that this type of corruption is often paired with more serious corruption.

Use of the term "computer hacking"

Evidence was given by a number of unions that their members did not fully understand how accessing confidential information from a system to which they had access could be a criminal offence called "computer hacking".[359]

The term "computer hacking", as it is used in popular culture, tends to conjure up images of a person from outside the agency breaking into a secure (restricted) computer system to cause damage to the

357 Evidence given by Professor Geraldine Mackenzie on 22 November 2019, p. 9.

358 Transcript of Ian Leavers dated 18 November 2019, p. 5.

359 Evidence given by Edmund Burke on 12 November 2019, p. 4.

agency's computer system or to obtain confidential information for financial gain. For example, there were media reports during 2017 and 2018 of the UK and other countries' health agencies' data being compromised or held to ransom by individuals attempting to extort money from the government.[360] This is obviously a different type of threat for agencies to deal with.

However, as demonstrated in this report, misuse of confidential information by employees can have significant consequences for the individual affected and the government agency involved. An offence provision in the Criminal Code specifically aimed at dealing with employees who improperly access confidential information is appropriate and will assist in making it clear that such conduct is not acceptable and can constitute a criminal offence.

Interpretation of "benefit"

Several prosecutions have been unsuccessful due to the interpretation of the term "benefit" [361].

Recently, in the District Court decision of *The Queen and Gerard Michael Neiland and Michael Andrew Neiland*,[362] Michael Neiland, a police officer, was charged with an offence of misconduct in relation to public office, an offence contrary to s. 92A of the Criminal Code[363]. Although the offence under consideration was not s. 408E, the issues that arose in this decision could be raised in a case involving s. 408E(2). It was alleged that Michael Neiland had accessed QPRIME to obtain information which he disclosed to his brother, Gerard Neiland, in relation to a drink driving conviction for another person.

In that case, Judge Richards determined that knowledge alone was insufficient to constitute a benefit. Even though Judge Richards acknowledged that "the definition [of benefit] is wide and it includes benefits without inherent or tangible value", she considered that "there must … be some benefit to be inferred or likely to follow". Judge Richards concluded that no benefit was derived because the information, namely the drink driving conviction, was available to the public at the time of the hearing and upon request through the court.[364]

The Criminal Code defines the term "benefit" in section 1:

> ***benefit*** *includes property, advantage, service, entertainment, the use of or access to property or facilities, and anything of benefit to a person whether or not it has any inherent or tangible value, purpose or attribute.*

The term "benefit" is further defined within s. 408E in subsection 5:[365]

> ***benefit*** *includes a benefit obtained by or delivered to any person.*

Professor Mackenzie commented on the first definition:[366]

> *... It is useful having that bigger definition in the Criminal Code that applies more generally but it has been difficult in some of the cases fitting benefit in there.*

---

360 https://www.abc.net.au/news/2017-05-13/ransomware-cyberattack:-technicians-work-to-restore-systems/8524170

361 s. 1, Criminal Code (Exhibit 108).

362 *The Queen and Gerard Michael Neiland and Michael Andrew Neiland*, Decision at Brisbane District Court on 26 August 2019 (Exhibit 158) 3-4.

363 Misconduct in relation to public office.

364 *The Queen and Gerard Michael Neiland and Michael Andrew Neiland*, Decision at Brisbane District Court on 26 August 2019 (Exhibit 158), pp. 3-4.

365 s. 408E of the Criminal Code (Exhibit 11).

366 Evidence given by Professor Geraldine Mackenzie on 22 November 2019, p. 6.

The Commissioner of Police echoed the frustrations encountered with the current provision:[367]

What is difficult, I supposed, for our agency is the interpretation of what benefit is.

Magistrate Simpson in the case of *Police and Stephen Thiry*, in consideration of s. 408E(2) of the Criminal Code, ruled that there was no benefit involved and concluded "It perhaps answers curiosity" when Mr Thiry, a police officer, had accessed the QPRIME database to obtain registration details and disclosed that information to a third party.[368]

Later that same year, knowledge was judicially determined as constituting a benefit in the *Police and Daniel Denis Banks*,[369] where Mr Banks accessed QPRIME on 23 occasions. During the searches Mr Banks obtained information about family members, friends and work colleagues as well as himself, including addresses and vehicle registration numbers.

There are three types of information which create difficulties in ascertaining if it is "information", as that term is used in s. 408E. The new provision should specifically include these types of information as being encompassed in the definition: [370]

- a person's own record
- publicly available information; and
- a search for information that is not found (for example, QPS surveillance of criminal activity).

Adequacy of sanctions

The penalties handed down for breaches of privacy are predominantly fines, as shown in table 4.[371]

Table 4: Penalties handed down for breaches of privacy

Case	Conduct	Outcome
DPP v Banks Ipswich Magistrates Court, 7 November 2017	Access	$4000 fine, no conviction recorded
Police v Betts Brisbane Magistrates Court, 14 March 2016	Access and disclosure	$8000 fine, no conviction recorded
Police v Binney Ipswich Magistrates Court, 22 November 2017 Note - applied for access, applied for disclosure	Access[372] and disclosure[373]	$1200 fine, conviction recorded
Police v McAnany Beaudesert Magistrates Court, July 2017	Access	$1500 fine, no conviction recorded
Police v Pryczek Rockhampton Magistrates Court, March 2018	Access	$2500 fine, conviction recorded
Neil Punchard[374] Brisbane Magistrates Court, 14 October 2019	Access and disclosure	Two months imprisonment, wholly suspended for a period of 18 months

367 Evidence given by Commissioner Carroll on 18 November 2019, p. 52.

368 *Police and Stephen Thiry*, Decision at Brisbane Magistrates Court on 6 March 2017, pp. 2-3.

369 *Police and Daniel Denis Banks*, Decision at Ipswich Magistrates Court on 15 September 2017 (Exhibit 155) 3.

370 Evidence given by Professor Geraldine Mackenzie on 22 November 2019, p. 15.

371 Table s. 408E Jurisprudence (Exhibit 160).

372 s. 408E Criminal Code.

373 s. 10.1 PS Act.

374 It is noted that there is currently an appeal awaiting determination in relation to the sentence given to Neil Punchard.

During her evidence, Professor Mackenzie spoke at length about the purpose of sentencing and how it works with respect to this provision. She covered the relevant sentencing guidelines, as contained in s. 9(1) of the *Penalties and Sentences Act 1992* (Qld).[375] Of greatest importance, the following was highlighted:[376]

> *In my view one of the most critical* [purposes for sentencing] *is to punish the offender to an extent or in a way that is just in all of the circumstances. And that's subsection (a), and that's about punishing in relation to the severity of the crime. That also brings in that element of public expectations and looks at all of the circumstances of the case.*

Professor Mackenzie went through three more relevant guidelines:[377]

> *…(c) is important to deter the offender or other persons from committing the same or a similar offence; (d) is about the community denouncing that type of conduct. Again, really important here. (e) is about protecting the Queensland community, and arguably that's important here as well, by punishing for those types of offences…*

The importance of general deterrence when sentencing for an offence under s. 408E of the Criminal Code is spelt out clearly in the commentary contained in *Carter's Criminal law of Queensland*.[378]

Professor Mackenzie summarised her view on the current jurisprudence:[379]

> *Depending on the severity of the matter and the fact that imprisonment hasn't yet been handed down, except a suspended sentence, this is under appeal, it does tend to send a message of lesser importance of these types of cases.*

With respect to the issue of whether the maximum sentence for offending under s. 408E should be increased, Professor Mackenzie was of the view that the most effective way Parliament could show that it is taking the offence seriously is through the maximum penalty it sets, which judicial officers must have regard to when sentencing. [380]

For example, s. 340 of the Criminal Code creates the offence of serious assault.[381] Pertinently, this aggravated form of assault includes any assault upon a police officer or public officer and provides for a maximum sentence of seven to 14 years, which is currently under review.[382] Professor Mackenzie opined that, akin to this additional protection provided to those public service employees, if public officers breach a member of the public's privacy then they should receive additional punishment.[383]

---

375 Exhibit 161.

376 Evidence given by Professor Geraldine Mackenzie on 22 November 2019 8.

377 Ibid.

378 Shanahan Ryan Rafter SC Costanzo Hoare, *Carter's Criminal law of Queensland 22nd Edition* (LexisNexis Butterworths, 2019) 636, quoting Studdert J at [54] in *R v Stevens* [1999] NSWCAA 69 and *R v Boden* [2002] QCA 164 (Exhibit 125).

379 Evidence given by Professor Geraldine Mackenzie on 22 November 2019 8.

380 Ibid 9.

381 Exhibit 165.

382 https://www.couriermail.com.au/news/queensland/queensland-government/more-jail-time-for-police-paramedic-prison-guard-assaults-ag/news-story/8783483073a249af87a0012a5c0f4d90.

383 Evidence given by Professor Geraldine Mackenzie on 22 November 2019 13.

Professor Mackenzie summarised her view on the maximum penalty and drafting of the current provision:[384]

> *But the most critical thing is detection and prosecution where appropriate and for Parliament setting the maximum as an indication of the seriousness of the offence. And that's always critical so that not only the courts have to look at that, but in terms of generally saying to the community, "This behaviour is wrong. There is a serious maximum penalty there and it must be taken seriously." But alongside that, and we've touched on that already, they have to believe that they're caught and they have to believe that what they're doing is actually a criminal offence and, therefore, the clarity of the provision becomes critical.*

A new offence was recommended by Professor Mackenzie, as amending the provision too much "*may inadvertently have the provision then become less useful in that hacking/viruses-type situation*". In addition, she considered that a new provision would be "*much more productive … mainly for the fact of sending that very clear message about the type of offending, that this is criminal behaviour and that you may not … access confidential information*". [385]

Analogous to s. 408E is the fifth special case in s. 398 of the Criminal Code, namely stealing by persons in the public service, where the maximum penalty increases from five years under s. 398(1) to 10 years.[386] Professor Mackenzie was of the view that an aggravating factor for misuse of confidential information should be when the offence is by a public officer, as defined in s. 1 of the Criminal Code.[387]

Public sector employees, and in particular police officers, are in a position of trust by virtue of their office. When public sector employees, and in particular police officers, misuse confidential information there is a loss of public confidence in the agencies concerned. The importance of general deterrence and need to punish particular offending more seriously was emphasised during the recent sentencing of Neil Punchard (see case study pages 42-43). Because of the position of trust held by police officers, particularly in circumstances involving vulnerable persons, this type of offending is particularly serious as it represents a significant breach of that trust.[388]

Professor Mackenzie also considered that another aggravating factor should be where the confidential information is disclosed to a third party:[389]

> *… I think that is one of the major problems with 408E as it currently stands, that disclosure isn't explicitly in that provision.*

The new offence would maintain the similar aggravating factor in s. 408E relating to circumstances where it could reasonably be anticipated that the misuse of information would facilitate the commission of a crime.

The proposed definition section clarifies that all information on the restricted database is confidential, even if publicly available elsewhere. It therefore prohibits users from accessing the database for purposes other than for those that are work-related. In addition, mere knowledge is encapsulated in benefit.

---

384 Ibid.

385 Ibid 10.

386 Exhibit 162.

387 Evidence given by Professor Geraldine Mackenzie on 22 November 2019 10; Exhibit 163.

388 *Police and Neil Glen Punchard*, Decision in Brisbane Magistrates Court on 14 October 2019, pp. 5-6.

389 Evidence given by Professor Geraldine Mackenzie on 22 November 2019, p. 11.

Recommendation for a new offence: "Misuse of confidential information by public officers"

Professor Mackenzie suggested the creation of a new offence which applies more generally, as contained in the new provision:[390]

> [Section 408E is] *based on the misuse of a computer and a restricted computer. It's not information more generally. So it doesn't apply if I pick up a piece of paper that I shouldn't have and act accordingly. It doesn't apply where I am told information in confidence and then use that information.*
>
> *…*
>
> *The type of concept we're really talking about here is breaching their duty of confidentiality and it is where it crosses the line between a breach of privacy under the [agency specific disclosure provision part of the] legislation and becomes criminal behaviour. I think any provision that's suggested does need to apply more generally, not just to public officers. Although public officers should be an aggravating factor. The key of a provision needs to be about the misuse of information, not just something on a computer, and allowing flexibility in what form that information takes.*
>
> *…*
>
> *I'd suggest taking away any requirement for restricted computer restricted data and so on and confidential information becomes the main point…- and also needs to apply in other cases where they're getting information verbally or in hard copy.*

Based on the above discussion, the CCC is recommending that a new criminal offence be introduced in the Criminal Code. The recommended offence has been drafted with the above-listed matters in mind, having regard to the overall message which is apparent from this analysis, namely that the current provision of s. 408E is not a sufficient deterrent to misuse of confidential information in the public sector.

The CCC notes that Profession Mackenzie's evidence recommended a new offence apply broadly to all employees with a circumstance of aggravation if the offence is committed by a public officer. The recommendation below has been limited to an offence which is committed by a public officer rather than any employee. The CCC has limited the recommendation to public officers because:

- the scope of Operation Impala was limited to the misuse of confidential information in the public sector
- the CCC has not examined the prevalence of misuse of confidential information outside the public sector, and
- the CCC has not consulted with other bodies which may have an interest in the creation of a new offence which would apply to all employees.

Whilst the recommendation of the CCC is limited to conduct by public officers, in the event that the legislature seeks to implement this recommendation, further consideration and consultation could occur to extend the operation of this offence to other employees.

390 Ibid, pp. 14-15.

Recommendation 10 – A new criminal offence

That the Criminal Code be amended to add a new offence of **misuse of confidential information by public officers**, to contain the following attributes:

1. Be divided into two parts, one relating specifically to misuse of confidential information on a computer and the other to provide for an offence misuse of any confidential information regardless of its source.
2. Access to the information is an offence where it was not in furtherance of the performance of a function of the agency.
3. The simpliciter offence which involves only access to the confidential information is to be a crime, punishable by 5 years imprisonment.
4. There are to be three aggravating circumstances to the simpliciter offence where the term of imprisonment increases to 10 years, namely:
    a. where the public officer or another person obtains a benefit, or
    b. when disclosure is made to a third party, or
    c. where access could facilitate the commission of a crime.
5. It is to be a defence if the access to the information was authorised, justified or excused by law.
6. The offence is to be added to the list of the indictable offences under s. 552A (1)(a) which must be heard and decided summarily on prosecution election.
7. The offence is to contain the following definition section:

    benefit includes:

    (i) obtaining knowledge of information from a database, or
    (ii) finding that there is no record in the database, or
    (iii) obtaining knowledge of information that is available from another public source

    computer includes any electronic device for storing or processing information

    confidential information includes all data, files and documents, irrespective of whether the information is publicly available from another source. The focus should be on the source of the information obtained as opposed to whether it could have been obtained lawfully via some other means.

Chapter 11 — Civil avenues of redress for victims

This chapter discusses and recommends a number of amendments to be made to Queensland's privacy legislation and related public sector practices currently in operation. The purpose of these amendments is to provide greater clarity in relation to information privacy principles and improve the protections and remedies available to victims who have had their confidential information unlawfully accessed and/or disclosed by public sector employees. Victims of these offences are often unaware of the breach, have limited remedies available to them, and then face a complex legal process to obtain a remedy or a compensatory award.

This chapter outlines discrepancies identified in Queensland's current privacy regime, in order to put the CCC's recommendations in context.

In reaching these recommendations, Operation Impala has had regard to and benefited from significant bodies of work carried out by the Australian Law Reform Commission (ALRC) into Commonwealth privacy legislation. The findings of the following ALRC Reports have been of particular assistance:

- Report 108: *For Your Information: Australian Privacy Law and Practice* (the 2008 ALRC Report); and
- Report 123: *Serious Invasions of Privacy in the Digital Era* (the 2014 ALRC Report).

The recommendations proposed by the 2008 ALRC Report helped significantly reform the *Privacy Act 1988* (Cth) (the Privacy Act) in 2014 via:

- the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) (the Enhancing Privacy Protection Act); and
- the *Privacy Amendment (Notifiable Data Breaches) Act 2016* (Cth) (the Notifiable Data Breaches Act).

The Enhancing Privacy Protection Act conferred new enforcement powers on the OAIC, and the Notifiable Data Breaches Act introduced a federal mandatory notifiable data breaches scheme (NDB scheme).[391]

Issues

The following key issues have been identified as particularly challenging for public sector agencies in the context of information security and privacy protection.

- The risk of under-reporting actual and potential misuse of confidential information
- Victims of misuse of confidential information not being notified proactively of breaches
- A failure to readily identify and report to the information regulator (the OIC) and/or victims affected, which has been signalled as an area that needs urgent improvement, given the detrimental impact this can have on individuals and public sector agencies more broadly

391 The explanatory memorandum of the Notifiable Data Breaches Act provides that the NDB scheme was supported by the recommendations of the 2008 ALRC Report in addition to the Parliamentary Joint Committee on Intelligence and Security's Advisory Report on the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (Cth) (see the Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill (2014), chapter 7).

- Uncertainty about obligations arising by virtue of the IPPs, in particular IPP4 [Storage and security of personal information][392] and reasonable steps agencies are required to take under the IP Act in furtherance of this principle
- A lack of enforcement powers of the OIC to conduct proactive investigations into privacy-related concerns involving public sector agencies, and
- A lack of availability and awareness of remedial avenues available to people who have had their confidential information misused.

Central advisory service to victim of privacy breaches

During the course of the public hearings, it was identified that the establishment of a central advisory service may be the most appropriate way to assist affected parties obtain assistance and identify avenues for relief.

The CCC heard from individuals affected by privacy breaches during the public hearings, including Renee Eaves who described feeling "frustrated", "extremely helpless" and "stressed" when trying to ascertain where to go to pursue appropriate remedial action.[393] She described the process as a "magical roundabout where it [the privacy complaint] ends up nowhere".[394]

Speaking in the context of matters involving domestic and family violence and making applications for remedies for victims of misuse of confidential information, Ms Eaves told the Commission:[395]

> *…It's the delays in that assistance that leaves, particularly in my view, women in a very vulnerable position, and it's that window where nothing is getting done and everybody's caught up in the red tape that the worst occurs.*

Another person affected by a privacy breach who gave evidence in a closed hearing described Queensland's privacy legislation and related processes as "inadequate" and "insufficient".[396] Philip Green, Privacy Commissioner, in his evidence described his exposure to privacy complaints and the impact that privacy breaches have on individuals, noting that "once something's known it can't become unknown…the impacts on the specific individual in a specific case cannot be underestimated".[397] Efforts are needed in Queensland to develop ways to provide information in a timely way to persons affected by privacy breaches.

Recommendation 11 – Central enquiry service

That OIC strengthens its enquiry service for victims who have had their confidential information misused, to include, if accepted, services outlined in recommendations 12, 14 and 15. Such services should include telephone and face-to-face advice delivery, with information available online, and scope to make referrals to other relevant agencies.

392 Schedule 1, IPA.

393 Evidence given by Renee Eaves on 19 November 2019, p. 8.

394 Ibid.

395 Ibid, p. 17.

396 Evidence given by de-identified witness on 26 November 2019, p. 41.

397 Evidence given by Philip Green on 22 November 2019, p. 26.

Extension and clarification of the Privacy Commissioner's powers and practices in Queensland

Mandatory NDB scheme for Queensland

At present, public sector agencies are under no obligation to notify the OIC or the affected victim/s in the event of a privacy breach. Queensland's current voluntary approach has been viewed as propagating under-reporting, weakening transparency and accountability, and impeding good practice.

The OAIC's *Notifiable Data Breaches Scheme 12-month Insights Report*[398] (NDB Scheme Insights Report) assesses the first 12 months of operation of the Commonwealth NDB scheme. The total data breach notifications for the preceding year were reported to have increased by 712 per cent compared with the previous 12 months under the voluntary scheme, with 86 per cent of breaches involving contact information disclosure as the most common form.[399] Harm-reduction strategies generated and implemented as a result included proactive audits of database access logs, enhanced password security requirements, multi-factor access authentication security measures, in addition to revised staff training packages to complement new practices.

The OIC submitted that a mandatory NDB scheme in Queensland, modelled on the Commonwealth regime (discussed in more detail below), would complement and bolster its existing audit and evaluation functions currently available under the IP Act and the RTI Act.[400]

The current government recommended in its *Review of the Right to Information Act 2009 and the Information Privacy Act 2009* that there should be further research and consultation to establish whether a mandatory NDB scheme in Queensland should be introduced.[401] In coming to that view, the government considered the OIC's submission titled *2016 Consultation on the Review of the Right to Information Act 2009 and the Information Privacy Act 2009*. In particular, the OIC noted that:[402]

> *…data breach notification is an important transparency measure for governments…that allow affected individuals to take remedial steps to lessen the adverse consequences that may arise from a data breach.*

During the Information Commissioner's evidence, the first year of operation of the Commonwealth NDB scheme was discussed,[403] having regard to the NDB Scheme Insights Report. One of the key messages from the NDB Scheme Insights Report was the "need for agencies to put individuals first".[404] The requirement to notify individuals of eligible data breaches was reported as incentivising entities to ensure reasonable steps are in place to adequately secure personal information.[405] As noted earlier in this report, unlawful disclosure of information about a member of the public's contact details (for example, address details) can have deleterious impacts on individuals and on public trust in government. The Information Commissioner, Rachael Rangihaeata, stated during her evidence:[406]

---

398 (2019), 20.

399 Ibid, 6.

400 OIC submission given to the CCC on 9 October 2019, p. 6 [30].

401 *Review of the Right to Information Act 2009 and the Information Privacy Act 2009*, Department of Justice and Attorney-General, Recommendation 13, p. 7.

402 2016 *Consultation on the Review of the Right to Information Act 2009 and the Information Privacy Act 2009* (2017) OIC, p. 51-52

403 Evidence given by Rachael Rangihaeata on 22 November 2019, 5.

404 OAIC (2019), Notifiable Data Breaches Scheme 12-month Insights Report, p. 20.

405 OAIC (2019), Notifiable Data Breaches Scheme 12-month Insights Report, pp. 2-3.

406 Evidence given by Rachael Rangihaeata on 22 November 2019, p. 5.

> *…It is important to note the impact of privacy concerns on trust…Government agencies collect and hold vast amounts of personal information as custodians on behalf of its citizens. And citizens trust and expect that the governments will use this responsibly and protect this information from unauthorised access, misuse and disclosure.*

The ALRC was supportive of national consistency being a goal of privacy regulation to lessen compliance burden and costs, to streamline information-sharing initiatives, and to give clarity to persons or entities wanting to make a privacy complaint. [407]

Having regard to possible issues concerning inconsistency between state and Commonwealth privacy legislation, the CCC is supportive of the OIC's submission that a Queensland NDB scheme, in addition to legislating own-motion powers (discussed below), "would provide Parliament, agencies, the community and OIC with assurance about agencies' legislative compliance and good practice". The OAIC's *Guide to securing personal information: "Reasonable steps" to protect personal information*[408] provides that the requirement to conduct a prompt and reasonable assessment of an eligible data breach may assist to reduce reputational risks for agencies and minimise other costs associated with data breaches.

It is envisaged an NDB scheme in Queensland would complement other risk-based reporting obligations stipulated by the Information Security policy IS18 2018, and otherwise voluntary requests for assistance by public sector agencies to the QGCIO as regards misuses of confidential information. Andrew Mills, Chief Information Officer, QGCIO, explained that whilst there is no requirement that agencies report instances of misuse of confidential information, agencies may request particular assistance from the QGCIO if such circumstances arise and are able to access support to better protect their systems. In addition, the IS18 policy requires agencies to develop information security management systems that detail how each system used by an agency will be protected, based on system usage.[409]

Victim notification in the event of a serious privacy breach

In consideration of the design of a mandatory NDB scheme in Queensland, the OIC submits that notifying victims in the event of a serious privacy breach will allow affected persons to take remedial steps to lessen the impact of adverse consequences, and is likely to prevent reoccurrence.[410] Results of a 2017 survey titled "Australian Community Attitudes to Privacy" showed that 95 per cent of people surveyed believed that if a government agency lost their personal information, they should be told about it.[411]

During Ms Rangihaeata's evidence, reference was made to the OIC's guideline on Privacy Breach Management and Notification[412] that outlines four steps for agencies to assist determine their response to privacy breaches.[413] Ms Rangihaeata spoke to the following four steps:

1. contain the breach
2. evaluate associated risks
3. consider notifying affected individuals, and
4. prevent recurrence.

---

407 ALRC (2008). 2008 ALRC Report, pp. 192-193.

408 OAIC (2018), *Guide to securing personal information: "Reasonable steps" to protect personal information*, pp. 3-4.

409 Evidence given by Andrew Mills on 20 November 2019, pp. 5-6.

410 OIC (2017), 2016 *Consultation on the Review of the Right to Information Act 2009 and the Information Privacy Act 2009*', p. 52.

411 OAIC, 2017, p. 16.

412 OIC (2018). Guideline: *Information Privacy Act 2009*, Privacy Breach Management and Notification (updated 1 February 2018).

413 Evidence given by Rachael Rangihaeata on 22 November 2019, pp. 6-9.

In particular, and as addressed in step 2, consideration of what type of information is involved in the breach may help agencies determine the likely harm to follow. Also, determining who is, or who may foreseeably be, affected by the breach becomes particularly significant at step 3, when deciding whether to notify affected individuals on this point. Ms Rangihaeata stated that:[414]

> *…it's not always a given that you should notify individuals. Sometimes it will cause more anxiety, particularly where you have a high level of confidence that you've contained the breach, or…you don't have a high level of certainty about who's affected.*

In the event of a serious breach of privacy that involves significant risks of harm to individuals, timeliness for agencies to act commensurate to the level of risk is of utmost importance. Being prepared "is really critical to achieving better outcomes for the community"[415]; it will lessen the timeframes of agencies when responding to breaches and notifying both the OIC and victims. It is anticipated this will have the dual effect of improving outcomes and reducing impact, reflected in the OIC's submission that provides:[416]

> *The requirements to notify individuals of eligible data breaches goes to the core of what should underpin good privacy practice for any entity—transparency and accountability. Being ready to assess and, if appropriate, notify of a data breach provides an opportunity for entities to understand where privacy risks lie within their operations…to prevent or minimise harm to individuals.*

Recommendation 12 – Mandatory Notification Scheme

That a mandatory data breach notification scheme be implemented in Queensland and that the OIC be responsible for developing the scheme, and receiving and managing the notifications.

Although there are existing requirements for agencies to respond within 45 days to a privacy complaint[417] the CCC considers it is important to continue to keep complainants updated with respect to any investigation into their complaint. Where such a complaint becomes subject to an investigation of corrupt conduct or misconduct, complainants should remain informed of the progress of the investigation. Updates to the complainant should of course be subject to any requirements to maintain confidentiality to protect the integrity of the investigation. Accordingly, the CCC recommends complainants be kept up to date with respect to the progress of the investigation.

Recommendation 13 – Updates to complainants regarding confidential information misuse complaints

That public sector agencies provide three-monthly updates to complainants regarding the management of their complaint, with sufficient details, where appropriate, regarding the progress and final outcome.

414 Ibid, pp. 8-9.

415 Ibid, p. 8.

416 OIC submission given to the CCC on 9 October 2019, p. 6 [29].

417 S. 166(3)(b) of the IP Act

Own-motion powers and declarations

Whilst the current privacy scheme in Queensland enables the investigation of non-compliance with the IP Act by way of a privacy complaint process, information obtained during the course of Operation Impala has signalled this regime as being insufficient to identify, adequately remediate and prevent incidents of misuse by public sector agencies.

The OIC has expressed concern with what it views as a "high threshold"[418] for the ability to issue a compliance notice if the Information Commissioner is satisfied a person has information relevant to assist their decision to give an agency a compliance notice or to mediate a privacy complaint.[419] Only if the conduct constitutes a serious or flagrant contravention of the agency's obligation to comply with the privacy principles, or the contravention has occurred on at least five occasions within the preceding two years, may the Information Commissioner have grounds to issue a compliance notice.[420] The OIC is of the view this limits the ability of the Information Commissioner to sufficiently investigate certain concerning acts or practices of an agency.[421]

There have been repeated calls for the OIC to have own-motion powers to investigate an agency or organisation engaged in conduct that may constitute an interference with the privacy of an individual. In 2017 in a submission to the Queensland Department of Justice and Attorney-General (DJAG), the OIC proposed a "contemporary legislative framework to manage new and emerging privacy risks".[422] The revised regime would equip the OIC with own-motion powers to investigate conduct proactively when considered desirable to prevent or mitigate misuses of confidential information, rather than merely reacting to such an incident after the fact.

The envisaged scheme would reflect the Commonwealth counterpart power.[423] The government was receptive to this proposal in principle, inserting the substance of the OIC's submission into Recommendation 19 of its responding Report[424], namely that the IP Act be amended to:[425]

> *…expressly provide the Information Commissioner with an "own-motion power" to investigate an act or practice which may be the breach of the privacy principles, whether or not a complaint has been made.*

The government's response was based on consultation with multiple public sector stakeholders, many in support of the OIC's proposal for own-motion powers. A consistent theme outlined in the government's response from those entities supportive of the proposal was that own-motion powers would assist to address systemic issues arising out of an act or practice of an agency. DoE and DoH were not in agreeance however, pointing to provisions of the IP Act[426] and the RTI Act[427] already in existence that were, in their view, sufficient in enabling the Information Commissioner to investigate matters subject to a compliance notice under the IP Act. Despite this, the government saw benefit in amending the IP Act to expressly provide own-motion powers to the Information Commissioner.[428] However, to date these recommendations are yet to be implemented.

---

418 '*2016 Consultation on the Review of the Right to Information Act 2009 and the Information Privacy Act 2009*' (2017) OIC, p. 54.

419 s. 197 of the IP Act.

420 s. 58 of the IPA.

421 '*2016 Consultation on the Review of the Right to Information Act 2009 and the Information Privacy Act 2009*' (2017) OIC, p. 53-54.

422 '*2016 Consultation on the Review of the Right to Information Act 2009 and the Information Privacy Act 2009*' (2017) OIC, p. 50.

423 s. 40(2) of the Privacy Act.

424 '*Review of the Right to Information Act 2009 and Information Privacy Act 2009*' (October 2017).

425 Ibid, p. 7.

426 s. 135.

427 s. 125.

428 DJAG response, p. 44.

The Commonwealth privacy regulatory regime has incorporated elements of the global standard, namely the EU General Data Protection Regulation 2016/679 (EU GDPR), including a number of useful enforcement capabilities that the Queensland system currently lacks and which are outlined below. In 2014, the Privacy Act was amended[429] to include "own-motion powers" by virtue of the Enhancing Privacy Protection Bill, which reads:

> *The Commissioner may, on the Commissioner's own initiative, investigate an act or practice if:*
>
> *(a) the act or practice may be an interference with the privacy of an individual or a breach of the Australian Privacy Principle 1; and*
>
> *(b) the Commissioner thinks it is desirable that the act or practice be investigated.*

[Note: the object of Privacy Principle 1—open and transparent management of person information—is to ensure APP entities manage personal information in an open and transparent way].

Declarations may be made by the Australian Information Commissioner after the investigation into a data breach[430]:

> *After investigating an act or practice of a person or entity under subsection 40(2), the Commissioner may make a determination that includes one or more of the following:*
>
> (a) a declaration that:
> (i) the act or practice is an interference with the privacy of one or more individuals; and
> (ii) the person or entity must not repeat or continue the act or practice;
> (b) a declaration that the person or entity must take specified steps within a specified period to ensure that the act or practice is not repeated or continued;
> (c) a declaration that the person or entity must perform any reasonable act or course of conduct to redress any loss or damage suffered by one or more of those individuals;
> (d) a declaration that one or more of those individuals are entitled to a specified amount by way of compensation for any loss or damage suffered by reason of the act or practice;
> (e) a declaration that it would be inappropriate for any further action to be taken in the matter.

Once the Privacy Commissioner has investigated a complaint and made an appropriate declaration, it would require referral to a court for enforcement.

The ability of the court to provide declaratory relief may be useful to give aggrieved persons official recognition that their privacy was breached and a sense of finality, and to avoid lengthy and costly court proceedings that may be re-traumatising. Victorian human rights barrister Sarala Fitzgerald gave evidence that supported the value of declarations "having teeth", having regard to a Victorian human rights charter case.[431] In that case, proceedings were brought with an accompanying human rights charter claim regarding a decision to reclassify an adult prison as a youth justice centre, which resulted in a number of children being detained alongside adult prisoners. Although the proceedings failed to reverse the original decision, the charter aspect survived and a declaration was made that confirmed the decision had breached the right of a child not to be subjected to inhumane or degrading treatment, particularly while deprived of liberty. This declaration significantly contributed

429 Via the insertion of s. 40(2).

430 Under s. 40(2), pursuant to s. 52(1A) of the Privacy Act.

431 Certain Children by their litigation guardian Sister Marie Brigid Arthur v Minister for Families and Children & Ors [2017] VSC 251 (11 May 2017).

to the removal of children from that facility, which demonstrates that a court's declaration that an individual's right to privacy has been breached can bring about "remarkable changes" with "powerful impact", despite there being no monies payable.[432]

The ALRC was supportive of the OAIC being enabled to make declarations. The 2014 ALRC Report recommendations included Recommendation 16—1, which reads:[433]

> *The Commonwealth Government should consider extending the Privacy Commissioner's powers so that the Commissioner may investigate complaints about serious invasions of privacy and make appropriate declarations. Such declarations would require referral to a court for enforcement.*

In the ALRC's view, declaratory relief would be beneficial to avoid inconsistencies that might arise if the Commissioner did *not* have a formal role in addressing serious invasions of privacy.

Additionally, a research article titled "The Privacy Commissioner and own-motion investigations into serious data breaches: a case of going through the motions?"[434] examined six high-profile matters that have been investigated since 2011 by the (Australian) Privacy Commissioner via own-motion powers. Of note, in March 2014 further enforcement powers were conferred on the Commissioner, including the power to:

- make determinations after an own-motion investigation
- seek a civil penalty in certain circumstances, and
- accept enforcement undertakings to take (or refrain from) actions to ensure compliance with the Privacy Act.

These additional powers were described as being able to "bring a deterrent and educative elements to those matters".[435] The (then) Acting Assistant Commissioner Compliance, Angelene Falk, commented that the new powers would provide credibility in furtherance of the enforcement of privacy law, which would operate as a greater incentive for privacy obligations and responsibilities to be taken seriously.

Having regard to that sentiment and the need for greater deterrence measures in the Queensland context, during the CCC public hearings the Privacy Commissioner, Philip Green, discussed possible improvements to the current privacy regulatory framework, with specific mention to his role being given own-motion powers. Mr Green commented that while "fines and penalties have their place…at the arsenal end", own-motion powers "would be an enhancement to this jurisdiction",[436] regardless of whether a matter was conciliated or proceeded to determination as to damages.

Ms Rangihaeata in her evidence highlighted the importance of maintaining societal trust in government as custodians of the community's personal information.[437] This echoes the findings of the NDB Scheme Insights Report, which encourages agencies to build an "individuals first" approach to privacy. Further, to adequately remediate the individual harm suffered by a privacy breach it would be beneficial for the OIC be able to make a declaration following an own-motion investigation.[438]

---

432 Evidence given by Sarala Fitzgerald on 19 November 2019, pp. 5-6.

433 2014 ALRC Report, 310.

434 Jodie Siganto and Mark Burdo (2015), *The Privacy Commissioner and Own-Motion Investigations into Serious Data Breaches: A Case of Going Through the Motions?* UNSW Law Journal, Vol 38(3), pp. 1145-1185 at p. 1174.

435 Interview with Angelene Falk, Acting Assistance Commissioner Compliance, OAIC (Sydney, 14 December 2012).

436 Transcript of Philip Green dated 22 November 2019, p. 9.

437 With reference to the OAIC "Australian Community Attitudes to Privacy Survey" (2017), p. (i).

438 Jodie Siganto and Mark Burdo (2015), The Privacy Commissioner and Own-Motion Investigations into Serious Data Breaches: A Case of Going Through the Motions? UNSW Law Journal, Vol 38(3), pp. 1145-1185 at p. 1175.

Recommendation 14 – Own-motion powers for the OIC

That the OIC have:

1. own-motion powers under the IP Act to strengthen existing powers and better identify systemic issues arising from an act or practice of an agency.
2. the power to make a declaration following an own-motion investigation, to be modelled on the comparable Commonwealth provisions.

Assistance in court proceedings

Operation Impala inquiries have revealed a number of challenges for individuals trying to pursue legal remedies as a result of a breach to their privacy. The key issues identified included:

- the length of court proceedings
- power imbalances between self-represented litigants, as compared to agencies' engagement of senior legal representation, and
- costs associated with court proceedings.

Renee Eaves, a person whose privacy was breached and a social justice advocate, told the CCC during her hearings evidence that QCAT is:

> *…timely, it's complicated. I've had a very big legal team assisting me on my matter, and quite frankly I've still found the process completely overwhelming.*

Ms Eaves also told the CCC she had been assisting a domestic violence victim with a matter that involved the misuse of confidential information. Ms Eaves explained this woman's experience as a self-represented litigant as being:

> *absolutely gruelling…instead of an apology and instead of simply reimbursing this victim for what it cost her to relocate her family on two occasions…the government are choosing now to continue to her…*[and] *the remedies are absolutely not sufficient because, in QCAT for start, it's capped as $100,000.*

Hearings evidence received from an anonymous witness (the domestic violence victim referred to above) who had her personal information disclosed, and at the time of the hearing remained involved in ongoing QCAT proceedings, referred to the process as "secondary abuse". The witness said during her evidence that:[439]

> *…The process has been very, very long….one goes to QCAT because you…expect it as they say on their website, to be efficient, time effective, not costly, quick and easy. And for somebody that's not a lawyer, the submissions I've needed to put together, self-represented, have taken a long time to put together. That's caused me hours, days, weeks, months and I'm still going through the process. This has been going on for two and a half years, and this has really caused a detriment to myself and my family.*

Currently, the Privacy Commissioner is able to refer a privacy complaint to QCAT in some circumstances.[440] However, the process is lengthy, involving initial consideration by the subject agency, attempts at mediation facilitated by the Information Commissioner, and the allowance of sufficient time for the matter to be heard and decided in QCAT, bearing in mind the appeal period.

439 Evidence given by an anonymous witness on 26 November 2019, p. 17.

440 pursuant to Chapter 5, Part 4 of the IPA.

During the Privacy Commissioner's evidence, there was a discussion of the OIC's potential to appear in QCAT proceedings as a friend of the court (*amicus curiae*) to provide impartial assistance to the court and make submissions on law where appropriate as a way to level an "imbalance of power".[441] When asked about how this approach would assist victims of privacy breaches, the Privacy Commissioner submitted that this approach would assist by providing more equal representation, and give greater scope for education and training regarding conciliation and court processes.

In the 2014 ALRC Report, it is recommended at the federal level that the Privacy Commissioner have new functions to 1) assist the court as *amicus curiae* where appropriate and with leave of the court, or 2) intervene in court proceedings on the same conditions being met.[442] It was suggested these additional functions would be similar to those conferred on other administrative bodies, such as the Australian Competition and Consumer Commission, the Australian Securities and Investments Commission and the Australian Human Rights Commission.

The OAIC in its submission to the issues paper to the 2014 ALRC Report, noted that *amicus curiae* and intervener roles would assist the management of complaints that relate to serious invasions of privacy.[443] Other jurisdictions have a right for the respective Privacy Commissioner to appear, be heard or joined as a party to proceedings, namely in New South Wales and Victoria.[444] The ALRC suggested that in the event a statutory cause of action was enacted for serious invasions of privacy, as also recommended in this CCC report, an increase in complaints referred to QCAT might bolster calls to enable the Privacy Commissioner as a friend of the court and/or represent the Information Commissioner's interests by way of an intervention function.

Recommendation 15 – Extending the role of the OIC in proceedings

That the OIC be able to appear as a friend of the court (*amicus curiae)*, and have the power to intervene in QCAT proceedings, where appropriate and with leave of the court.

QCAT resourcing and compensation under the IP Act

Evidence provided to Operation Impala included reference to QCAT's current extensive backlogs. Renee Eaves gave evidence that her matter against the QPS was lodged with QCAT in 2016, with an initial determination made in June 2018; she is waiting for an appeal to be heard in 2020.[445] Ms Eaves also spoke about another matter against the QPS involving delays of 39 months thus far.[446]

The CCC acknowledges there may be an increase in the number of matters before QCAT with the advent of own-motion powers for the Privacy Commissioner. Irrespective of any potential additional workload, the CCC considers that it would be beneficial for victims if there were to be provision of additional resources to QCAT, namely additional hearings rooms and members to help alleviate the possible additions to workload. This echoes what has already been flagged in the 2017–2018 QCAT Annual Report, which provides that "without additional funding—which has been sought—backlogs in this jurisdiction will climb".[447]

441 Evidence given by Philip Green on 22 November 2019, pp. 4-5.

442 The 2014 ALRC Report, p. 317.s

443 OAIC submission 66, ALRC Discussion Paper, Serious Invasions of Privacy in the Digital Era, 30 March 2014.

444 *Privacy and personal Information Protection Act 1988* (NSW), s. 55(6); *Privacy and Data Protection Act 2014* (Vic), s. 74.

445 Evidence given by Renee Eaves on 19 November 2019, p. 16.

446 Evidence given by Renee Eaves on 19 November 2019, p. 15.

447 Queensland Civil and Administrative Tribunal, p. 18.

It is noted that every magistrate is taken to be a member of QCAT for minor civil disputes, [448] capped at $25,000. In effect, magistrates are empowered to assist with some of QCAT's current backlog (albeit limited to minor civil disputes only). In addition, magistrates may be appointed as supplementary QCAT members for stated periods.[449] It would be beneficial to victims if this provision could be used to enable QCAT's current extensive backlogs to be dealt with in a timely manner.

An increase to QCAT's compensation limit for IP Act matters would further assist victims in this jurisdiction. The current QCAT limit on compensation under the IP Act is $100,000. The CCC notes the suggestion of the Queensland Human Rights Commissioner of a compensation limit commensurate to the non-economic loss in defamation, which is currently $407,500.[450] Given magistrates are enabled to hear QCAT applications, the CCC suggests the IP Act damages limit be amended to reflect the Magistrates Court jurisdictional limit of $150,000.

Strengthening the protections to victims afforded by the IP Act

IP Act privacy principles

There are eleven privacy principles contained in Schedule 3 of the IPA. Agencies must comply with these principles and a breach of any of them can give rise to a privacy complaint which is initially dealt with by the Privacy Commissioner and then QCAT, if it remains unresolved, as discussed above.

The main privacy principle discussed throughout Operation Impala was IPP4, which deals with the storage and security of personal information.

Section 178 of the IP Act gives rise to a cause of action against the agency for failing to comply with IPP4. The initial privacy complaint is made to the Information Commissioner. Referral of the complaint to QCAT applies under Part 4 of the IP Act, in circumstances where it is unlikely that the Information Commissioner will effect resolution through mediation or a mediation has taken place which has been unsuccessful.[451]

IPP4 provides:[452]

(1) An agency having control of a document containing personal information must ensure that-
  (a) The document is protected against-
    (i) Loss; and
    (ii) Unauthorised access, use, modification or disclosure; and
    (iii) Any other misuse; and
  (b) If it is necessary for the document to be given to a person in connection with the provision of a service to the agency, the agency takes **all reasonable steps** to prevent unauthorised use or disclosure of the personal information by the person.

448 s 171(2) QCAT Act.

449 s 192(1) QCAT Act.

450 Submission given by Queensland Human Rights Commissioner on 3 December 2019, p. 5.

451 IP Act s 174.

452 *Information Privacy Act 2009* (Qld) Sch 3.

The NPPs regulate health agencies. They are similar in content to the IPPs and are contained in schedule 4 of the IP Act.

NPP4 provides:[453]

(1) A health agency must take reasonable steps to protect the personal information it holds from misuse, loss and unauthorised access, modification or disclosure.
(2) If the personal information is no longer needed for any purpose for which the information may be used or disclosed under NPP2, the health agency must take reasonable steps to ensure that the individual the subject of the personal information can no longer, and can not in the future, be identified from the personal information.

The term "reasonable steps" is not defined for either the IPPs or NPPs and has given rise to litigation in QCAT, where self-represented victims have found themselves up against agencies represented by large and experienced legal teams.

Overview of the *Human Rights Act 2019* (Qld) and relevant implications

The introduction last year of a Human Rights Act in Queensland has a number of ramifications for privacy complaints by victims against agencies including:

(a) The legislation protecting victims' privacy must be compatible with human rights; and

(b) Victims can add a human rights claim onto a privacy claim in court where an agency has breached the victim's human rights.

Only two other jurisdictions in Australia have human rights acts: the *Human Rights Act 2004* (ACT) and the *Charter of Human Rights and Responsibilities Act 2006* (Vic) (*Vic HR Act*).

The Queensland HR Act was passed on 27 February 2019. The Anti-Discrimination Commission Queensland transitioned to the Queensland Human Rights Commission (QHRC) on 1 July 2019. The remaining functions and obligations under the HR Act commenced on 1 January 2020.

The right to privacy is one of the 23 protected human rights, which specifically entails that:[454]

> *A person has the right-*
> *(a) Not to have the person's privacy, family, home or correspondence unlawfully or arbitrarily interfered with.*

The HR Act aims to build a culture in the Queensland public sector that respects and promotes human rights.[455]

Public entities include public service employees and members of the QPS.[456] Agencies must act and make decisions in a way that is compatible with human rights. [457] It is unlawful for a public entity to:[458]

- to act or make a decision in a way that is not compatible with human rights or
- in making a decision, to fail to give proper consideration to a human right relevant to the decision.

453 *Information Privacy Act 2009* (Qld) Sch 4.

454 HR Act s 25(a)-(b).

455 Ibid s 3(b).

456 Ibid s 9(1)(a)-(c).

457 Ibid s 4(a)-(b).

458 Ibid s 58(1)(a)-(b).

However, a human right can be limited if the agency can prove that it is reasonable having regard to certain factors listed in the HR Act.[459]

The CCC may, with the consent of the person entitled to make a human rights complaint, refer the complaint to the QHRC when it considers the complaint may also be a human rights complaint.[460]

The QHRC has investigatory and mediatory functions, including compulsory conciliation, under the HR Act in relation to human rights breaches. A complaint must be made to the agency in the first instance, and after a period of 45 days a complaint may be made to the QHRC. The QHRC prepares reports for all complaints which remain unresolved, which must include the substance of the complaint and the actions taken to try to resolve the complaint, and may include recommendations for the agency to ensure compatibility with human rights.[461]

Although there are not any damages available for a breach of a human right, an individual is able to "piggy-back" the human rights breach onto an existing claim involving an independent claim (cause of action) against a public entity, and seek a declaration as discussed above.[462]

IP Act privacy principles – compatible with the HR Act?

The CCC inquiries resulted in a determination that the current IP Act privacy principles are in need of updating to provide more protection to the public by more stringent requirements being placed on agencies to protect the public's confidential information.

From a human rights perspective, Victorian legislation can be compared and followed as the Vic HR Act is based on similar legislation in the United Kingdom, [463] and on the International Covenant on Civil and Political Rights (ICCPR) (to which Australia is a party).

The ICCPR refers to a right to privacy in terms similar to those in the HR Act:[464]

> *No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence…*

The Explanatory Notes to the IP Act make no reference to consideration being had in drafting the IP Act to ensure that the act is compatible with the human rights and freedoms recognised or declared in the international instruments listed in s. 3(1) of the *Human Rights (Parliamentary Scrutiny) Act 2011* (Cth) when discussing the IP Act's consistency with legislation of other jurisdictions, which includes Article 17 of the ICCPR.[465] In contrast, the explanatory memoranda for the current Commonwealth and Victorian information privacy Acts explicitly state that they are compatible with human rights. [466]

Both the Queensland and Victorian IPPs are based on the Commonwealth NPPs. Commonwealth and Victorian law have evolved since the enactment of the NPPs; whereas the Queensland law has not. As amended by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth),

---

459 Section 13 HR Act.

460 HR Act s 66(1)(c) and (2)(b).

461 HR Act s 88(3)-(4).

462 Explanatory Notes, Human Rights Bill 2018 (Qld) 8 [2].

463 Human Rights Act 1998 (UK).

464 International Covenant on Civil and Political Rights, opened for signature on 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) art 17 ('ICCPR').

465 Explanatory Notes, Information Privacy Bill 2009 (Qld), p 7 paras 5-6.

466 Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth), p 44; Explanatory Memorandum, Privacy and Data Protection Bill 2014 (Vic), p 7.

Commonwealth regulation of privacy is carried out under s. 14 and sch. 1 of the *Privacy Act 1998* (Cth) in accordance with APPs as recommended by the 2008 ALRC Report.[467]

The Queensland Human Rights Commissioner, Scott McDougall, considers that the IP Act may require amendment in order to be compatible with the HR Act.[468] Further, he recommends:[469]

> *The right to privacy under the* [HR Act] *may require public entities to have adequate procedural safeguards against unauthorised access and disclosure of stored personal information … It will not be sufficient for public entities to only have policies in place; they must also take reasonable steps to ensure the policies are followed. Failure to provide adequate safeguards may amount to a disproportionate and therefore unlawful limitation of a person's right to privacy. Matters that may need to be considered include how information is stored, duration, usage, access by third parties, procedures to preserve the integrity and confidentiality of data, and procedures for destruction.*

Both the Commonwealth and Victorian privacy principles provide for the destruction of information, namely Principles 11.2 and 4.2 respectively; whereas neither IPP4 nor NPP4 provide for such protection.

When discussing gaps in Queensland's privacy principles as compared to the Victorian principles, Ms Fitzgerald noted the added protections in the Victorian principles with respect to anonymity, unique identifiers and sensitive information which Queensland does not currently have, although the Commonwealth's APPs do.

The OIC's submission strongly advocated for reform to the IP Act:[470]

> *It is the OIC's view that existing provisions in the IP Act require strengthening to provide adequate remedies for individuals who have had their privacy breached by public sector agencies….*

Mr Green recommended:[471]

> *… we should merge the NPPs and IPPs into a version that follows the Federal jurisdiction.*

Specifically in relation to the definition of "reasonable steps" in IPP4 and NPP4, Mr Green explained that:[472]

> *… the best pronouncement is … the GDPR which is almost the global standard now in this area and it has an Article 32 which has a very fulsome definition.*
>
> *The GDPR … is the General Data Protection Regulation that's been enacted in and adopted in Europe. … GDPR has had the benefit, I guess of quite a lot of European experience on privacy and a lot of input. A lot of countries are looking at that and indeed the ACCC, I think, has followed some of the law there and its recommendations on Australian law reform.*

---

467 Australian Law Reform Commission, For Your Information: Australian Privacy Law and Practice, report 108 (vol 1) (2008) 34-48, recommendations 18-31.

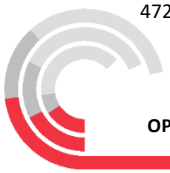
468 Ibid 5.

469 Ibid 3 [10] and 6 [27].

470 Ibid 8 [2].

471 Transcript of Philip Green dated 22 November 2019 6 [1] and Exhibit 178 (GDPR and IS18).

472 Ibid 6-8.



> *… the GDPR … I think it's quite relevant to what agencies should be expected to apply in terms of what's reasonable.*
>
> … [when compared to the Queensland Government Chief Information Office's information security policy (IS18:2018)] *… the European one has better wording in terms of appropriate technical and organisational measures to ensure a level of security appropriate to the risk…*
>
> … [Article 32 of the GDPR is] *probably a standard we should aspire to …*

Mr Green explained that the Commonwealth privacy legislation (including the APPs) is based on the European model and summarised the difficulties faced within Australia by the existence of differing privacy regimes, and in particular Queensland having both the IPPs and NPPs:[473]

> [Article 32 of the GDPR is the] *regime in EU, which the Australian one is based on largely… I'd say if Queensland … was to enact the regime … it should follow the Australian one, just for a consistency perspective particularly where agencies operate across jurisdictions. And to help avoid confusion … the national privacy principles in Queensland can confuse people. They apply to health agencies currently. So there can be confusion particularly if there's differing timeframes or different regimes.*

The OIC, in its 2017 submission to DJAG at recommendation 14 submitted that the definition of "personal information" in the IP Act be amended to be consistent with the Commonwealth definition.[474] In October 2017 the Government provided a response, concurring that this definition as contained in section 12 of the IP Act should be so amended from:

> *…information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.*

to the same as section 6 of the Privacy Act (Cth):

> *information or an opinion about an identified individual, or an individual who is reasonably identifiable:*
>
> (a) whether the information or opinion is true or not; and
> (b) whether the information or opinion is recorded in a material form or not.

The Government response noted that when the IP Act was drafted the definition of "personal information" mirrored the definition in the Commonwealth act, which was subsequently amended; whereas the Queensland act was not also updated.

The 2014 ALRC report, enunciated nine guiding principles, including that Australian privacy laws should meet international standards,[475] and that privacy laws should be coherent and consistent throughout Australia.[476]

---

473 Ibid 14.

474 *'2016 Consultation on the review of the Right to Information Act 2009 and Information Privacy Act 2009'.*

475 Australian Law Reform Commission, Serious Invasions of Privacy in the Digital Era (2014) 35.

476 Ibid 37.

In the 2008 ALRC report, relevant to the current Queensland privacy legislation, is recommendation 18:[477]

> ***Recommendation 18-2***
> *The Privacy Act should be amended to consolidate the current Information Privacy Principles and National Privacy Principles into a single set of privacy principles*

Recommendation 16 – A single set of privacy principles

That the IPPs and NPPs in the IP Act be amalgamated and strengthened, having regard to the APPs contained in the Privacy Act (Cth); and in particular the:

1. definition of "reasonable steps" in the fourth of each set of principles relating to security of data be further defined in accordance with the terms of Article 32 of the EU GDPR; and
2. definition of "personal information" be amended in the IP Act to accord with the current version contained in the Privacy Act (Cth).

New statutory tort for privacy breaches

The main avenue for victims of privacy breaches to claim against the offending agency is through QCAT by way of a claim under the IP Act, as discussed above. This process is the entry level avenue of civil redress.

Given that the new HR Act allows victims to add on a human rights claim to another court action, there has been renewed interest in Queensland in looking into the different potential claims, or causes of action, that victims can make through the courts. These processes present as more sophisticated avenues for victims but are nonetheless extremely useful tools in a victim's arsenal against an agency that has breached their privacy.

Presently, the options are extremely limited and hence, the introduction of a concrete new cause of action would be of great assistance to victims.

The only other civil cause of action is one that is barely known by the public, and much less used by them. It is entitled equitable breach of confidence. Moreover, breach of confidence actions for misuse of confidential information are problematic with respect to the available remedies. The basis on which equity can award compensation, by way of common law compensatory damages and aggravated damages, for emotional distress arising from the breach of a purely equitable wrong is unclear.[478] There is only one decision at appellate level, from Victoria, for the recovery of compensation for emotional distress in a breach of confidence action.[479]

Professor Barbara McDonald, a torts expert, emphasised during her hearings evidence that an equitable action for breach of confidence depends on the extent of the misuse of the information. She queried whether instances of breaches born out of curiosity without personal use of the information or disclosure to a third party would be sufficient to found a claim under this cause of action.[480]

---

477 Australian Law Reform Commission, For Your Information – Australian Privacy law and Practice (2008) 34.

478 Australian Law Reform Commission, Serious Invasions of Privacy in the Digital Era, Report 123 (2014) 269.

479 Giller v Procopets (2008) 24 VR 1.

480 Evidence given by Professor Barbara McDonald on 15 November 2019 16 [5].

The legal term "equitable action" refers to a civil claim which arises to fill the gap in the law. There exists a huge gap in the current law of tort, which requires rectification. It is far from ideal that for a member of the public to seek compensation from an agency for misuse of their confidential information they have to resort to pursing the difficult claim in equity.

Current state of the law of tort for privacy breaches

In law, a "tort" means a civil wrong, namely a breach of a duty imposed by law. Tort law is concerned with compensation for damages for civil wrongs suffered as a result of another's acts or omissions. There does not currently exist a tort of privacy in Australia. Common law, derived from judicial precedent (case made law), remains the main contemporary source of the law of tort.

A number of Australian decisions have paved the way for the acceptance of the tort of privacy.[481] In 2001, the High Court held that there was no authority preventing the development of a tort of invasion of privacy in Australia.[482] Two lower court decisions have recognised a tort of privacy, in Queensland[483] and Victoria.[484] Both matters did not reach the appellate level. The cases suggest that the future development of the common law is, at best, uncertain.[485] Judges take an incremental approach to the expansion of existing causes of action to cover novel situations, rather than creating a new tort altogether.[486] Therefore, it is unlikely that the common law will evolve to the degree required in the area of privacy breaches, which is not a new problem.

Australia is behind many other countries where statutory torts for privacy breaches exist, including New Zealand, the United Kingdom, several Canadian provinces and several states in America. [487]

One of the two types of invasion of privacy for an action in tort recommended by the 2014 ALRC Report was for misuse of private information. Misuse of private information includes disclosure.

The 2014 ALRC Report summarised the benefits of a statutory tort as opposed to one developing at common law:[488]

- a statute can legislate for a range of situations, both for what has occurred in the past and may occur in the future;
- there is more flexibility in the development of the law as opposed to the common law;
- statutes can select the most appropriate elements of a cause of action; and
- statutes can address complex policy issues and legal concepts.

For these reasons the CCC called Professor McDonald to give evidence during the public hearings. Professor McDonald is a tort expert, who was appointed Commissioner in Charge for the ALRC Inquiry into Serious Invasions of Privacy in the Digital Era. The resulting report, the 2014 ALRC Report, made several recommendations which included a new Commonwealth statutory tort for serious invasions of privacy for two types of invasion. One of the two types of invasion was the "*misuse of private information, such as by collecting or disclosing private information about the plaintiff*".[489] The enactment of a statutory tort by the Commonwealth has not occurred, despite

481 Richards Ludlow Gibson, Tort Law in Principle 5th Edition (Thomson Reuters (Professional) Australia Limited, 2009) 17.

482 Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd (2001) 208 CLR 199.

483 Grosse v Purvis [2003] QDC 151.

484 Doe v Australian Broadcasting Corporation [2007] VCC 281.

485 Australian Law Reform Commission, Serious Invasions of Privacy in the Digital Era, Report 123 (2014) 55.

486 Richards Ludlow Gibson, Tort Law in Principle 5th Edition (Thomson Reuters (Professional) Australia Limited, 2009) 16.

487 Australian Law Reform Commission, Serious Invasions of Privacy in the Digital Era, Report 123 (2014), p 81.

488 Ibid 24.

489 Australian Law Reform Commission, Serious Invasions of Privacy in the Digital Era, Report 123 (2014) Rec 4-1 & 5-1(b).

several other similar recommendations being made in various reports and during other inquiries, as recently as June 2019.[490]

Proposed new statutory tort

The recommendation in this report adopts the proposal contained in the 2014 ALRC Report, namely the enactment of a statutory cause of action for serious invasions of privacy to provide for a cause of action where there has been a misuse of private information. The CCC recommends the enactment be at the state level in Queensland. Whilst it is preferable, having regard to consistency across Australia, simplicity and efficiency,[491] for the Commonwealth to enact the new statute, where the Commonwealth continually fails to act despite several inquiries recommending the same then Queensland should lead the way:[492]

> *I think in the absence of a Commonwealth Act then it is up to the States to take action.*

Professor McDonald explained how her design of the action set out available remedies and that a statutory tort does not have to be limited to common law tort remedies:[493]

> *There might be other things such as an account of profits, for example, a take-down order in respect of internet invasions which could be catered for in the legislation itself.*

Professor McDonald summarised the preferred content of the new statute:[494]

> *And I'm also very much in favour, obviously, that if a statutory action is to be enacted it should be as precise in terms of its protections as is appropriate. I'm not in favour of the view that certain fundamental features of a statutory cause of action should be left up to the courts to decide, because the courts need guidance from a legislature as to their Parliamentary intention.*

Lastly, Professor McDonald confirmed that during the 2014 Inquiry advice was sought which confirmed there exists the constitutional power to enact a statutory tort.[495]

Philip Green, Privacy Commissioner, echoed Professor McDonald's recommendation that a statutory tort for privacy breaches be enacted:[496]

> *I support fully consideration of the tort or a statutory cause of action* [of serious invasion of privacy misuse of information] *as it's been recommended by the Law Reform Commission and ACCC.*

Mr Green considered that a statutory tort of privacy would be a useful remedy to have available. He also attested to its potential to help develop privacy protection through its deterrent effect, which would likely encourage agencies to ameliorate their internal practices. Mr Green noted that there

---

490 Australian Law Reform Commission, For Your Information: Australian Privacy Law and Practice, Report 108 (2008) Rec 74-1; NSW Law Reform Commission, Invasion of Privacy, Report 120 (2009) [4.14]; Victorian Law Reform Commission, Surveillance in Public Places, Report 18 (2010; 'A Commonwealth Statutory Cause of Action for serious Invasion of Privacy' (Issues paper, Department of the Prime Minister and Cabinet, 2011); and Australian Competition and Consumer Commission, Digital Platforms Inquiry, Report (2019) Rec 19.

491 Evidence given by Professor Barbara McDonald on 15 November 2019 6 [3].

492 Ibid 8 [4].

493 Ibid 7 [1].

494 Ibid 8 [6].

495 Ibid 9 [5].

496 Evidence given by Philip Green dated 22 November 2019, p 20.

are higher damages available for breach of a tort when compared to the $100 000 limit in QCAT for breach of the IPPs. Mr Green commented that there exist "severe penalties" for breaches of privacy in Europe. On account of the legal representation costs involved in pursing such a claim, Mr Green considered that it was not "a panacea necessarily but it could be an additional benefit".[497]

Recommendation 17 – Statutory tort for misuse of private information

That the Queensland Government consider the introduction of a statutory tort for serious invasion of privacy by the misuse of private information, such as by collecting or disclosing private information about the plaintiff, as described in the ALRC 2014 Report.

Agency liability for employees' misuse of confidential information

Throughout the course of the public hearings it became evident that complacency exists in some agencies in ensuring sufficient safeguards are in place to secure the public's confidential information. The evidence of expert witnesses also highlighted current gaps in agency service delivery.

This problem is not Queensland specific. Ms Fitzgerald explained that the precipitating factor for the amendment of the *Information Privacy Act 2000* (Vic) to the *Privacy and Data Protection Act 2014* (Vic) was the 2009 report by the Victorian Auditor-General entitled *Maintaining the Integrity and Confidentiality of Personal Information*. Ms Fitzgerald discussed pertinent portions of the report. The report found that public sector agencies were not managing data well. The amending legislation introduced a more rigorous regime for the management of data and use of information held on databases. As agencies were not taking steps to ensure that their data was protected, the legislature stepped in to force them to do so.

Recommendations included:[498]

- a comprehensive, integrated suite of standards and guidance that address all aspects of information security
- staff training on the importance of information security
- regular monitoring of staff compliance with information security policies and standards
- assessment of both internal and external threats and vulnerabilities
- regular monitoring of access controls
- regular monitoring of access logs
- random checks of controls of receiving agency when information sharing

Operation Impala found that the agencies it examined were, to varying degrees, providing insufficient protection to the confidential information they held on behalf of the public.

The advent of the HR Act, allowing a victim to add a human rights claim onto an existing claim in court will likely lead to increased litigation by members of the public. In order to defend to those claims agencies will need to improve their internal systems.

497 Evidence given by Philip Green dated 22 November 2019, p 21.

498 Victorian Auditor-General, Audit Summary of Maintaining the Integrity and Confidentiality of Personal Information, 25 November 2009 (Exhibit 127).

With respect to the ability for human rights claims to be joined to existing causes of action, Scott McDougall, Queensland Human Rights Commissioner, cautioned agencies:[499]

> *And it's often referred to as the piggy-back provision. So it entitles a person who has an existing standalone cause of action to attach their human rights argument to that cause of action … it is not entirely toothless and I expect that it will be used and we will see jurisprudence develop in Queensland by that provision.*

In his submission Mr McDougall examined international authority prior to concluding:[500]

> *The implementation of the* [HR Act] *is an opportunity to revisit the purpose and importance of privacy when dealing with confidential information and provide an ethical framework that supports fair decision-making, where individual rights are considered and balanced against organisational need and efficiency. A genuine commitment to this approach cannot be achieved through policy alone. Policies need to be supported by understanding and leadership from senior officers, and training for all staff.*

Further to the measures recommended throughout this report, a detailed explanation of agency liability for employee misuse of confidential information is considered to be of assistance to agencies. This is because throughout Operation Impala it was apparent that agencies tend to minimise their liability for their employees' actions, most notably the QPS in the matter involving Mr Punchard (See case study pages 42-43 and discussion below).

Personal liability of agencies for public officers

Agencies can be held personally liable for their employees' actions. To avoid such liability, agencies must take reasonable steps — for example, in the case of misuse of confidential information, by ensuring that their stored information is adequately protected.

Professor McDonald provided some guidance on what are "reasonable steps" for agencies to take to avoid being personally liable:[501]

> *[Personal liability] means failing to have proper processes. It is a little bit analogous to an employer who has to provide a safe system of work for an employee. You have got to provide proper equipment, proper methods, systems for protection in terms of software and hardware, you'd have to be reasonably available and affordable I suppose security systems, up-to-date security systems. You'd have to have training of staff, supervision of staff, selection of staff. You'd have to follow-up reports of problems, you'd have to have disciplinary consequences and so on.*
>
> *So an employer, therefore, is charged with supervising and ensuring taking* ***reasonable steps****…And if the employer fails to do any of those things they would be* ***personally liable****….That's quite separate to vicarious liability…*

QCAT handed down a decision on 27 March 2019,[502] where the QPS was found to be personally liable, having breached IPP4 by failing to take "*all reasonable steps to prevent Senior Constable Punchard's unauthorised use or disclosure of ZIL's personal information*".[503]

499 Ibid 8.

500 Ibid 3 [10] and 6 [27].

501 Evidence given by Barbara McDonald on 15 November 2019, 17 [5]-[6].

502 ZIL v Queensland Police Service [2019] QCAT 79.

503 Ibid [57].

The unauthorised access and disclosure, constituting an offence under s. 408E(2) of the Criminal Code, to which Mr Punchard pleaded guilty on 14 October 2019, involved Mr Punchard providing ZIL's residential address to her ex-partner.[504] The breach of privacy was not detected by the QPS but by ZIL and not until over two years later in May 2016. ZIL stated during the proceeding that she was a victim of domestic violence.

QCAT made the following findings concerning the failings of the QPS with respect to reasonable steps:[505]

> *Senior Officer Doogan gave evidence that there are various levels of access to the QPrime system…*
>
> *So we have an identifiable group of Queenslanders, those who are the subject of domestic violence orders, and I'm imagining your system is able to run a search that pulls up those people? ---Yes.*
>
> *But there is no safeguard to their information in any different way to somebody looking at someone who doesn't have a domestic violence order? ---All of the information is classified as protected, within the database…*
>
> *Detective Inspector Prestige also gave evidence. His evidence was that he was not aware of any random audits of QPrime in use in his 25 years of service.*
>
> *The evidence before me is that the QPS had no systematic auditing procedures of access to the QPrime system – even for at risk groups such as domestic violence victims. It simply relied on either a complaint or an incident to highlight a breach of the QPrime system. This system of auditing after the fact allows for circumstances where catastrophic events involving ZIL and the safety of her family could have occurred based on knowledge taken from the QPS's own data system by a traffic officer for a childhood friend.*

From the matter of ZIL, being only one of two matters where QCAT has made an award of financial compensation order against an agency,[506] it appears that an agency with a fully auditable database system is obliged to conduct audits of accesses at least on a random basis.

This conclusion is reinforced in the recent appellate decision in ZIL, refusing the QPS leave to appeal out of time.[507] With respect to the prospects of a successful appeal, QCAT summarised the reasons supporting the tribunal at first instance's determination that the QPS was personally liable in that the QPS had breached its own duty of care to ZIL by failing to maintain a system which would have prevented, or at least deterred, delinquent officers from violating the Information Privacy Act.[508]

In this decision, the historic matter of *Rook v Maynard* (1993) 70 A Crim R 133 was quoted with respect to the requirement for the QPS to conduct audits of QPrime, concluding that monitoring systems are not infallible but they are an effective deterrent:[509]

> *There is nothing particularly novel about monitoring systems for computers storing confidential data.*

504 Ibid [1]-[5].

505 Ibid [33][34]&[50].

506 Office of the Information Commissioner submission received 9 October 2019 [35].

507 QPS v ZIL [2019] QCATA.

508 Ibid [13].

509 Ibid [18].

Philip Green was firm in his view that an agency should be undertaking regular audits and regular review of the audits to satisfactorily comply with "reasonable steps" at the most basic level.[510] In addition, he emphasised that proactive audits are an "absolutely critical" step for every agency when looking at an agency's compliance with reasonable steps, in order to protect its data from misuse in compliance with IPP4 and NPP4.[511]

Vicarious liability of agencies for public officers

Vicarious liability means that agencies can be held liable for their employees' conduct committed in the course of their employment. This type of liability is "strict" or absolute liability.[512]

The liability of the employer is based in policy to deter wrongful actions by employees:[513]

> *the encouragement provided by vicarious liability to employers to institute proper safety standards within the enterprise, so that vicarious liability is consistent with a theory of deterrence.*

The legal test for determining whether or not the tort is committed in the course of employment is: [514]

> *Was the employee carrying out the work he or she was employed to do, taken in the context of all surrounding circumstances?*

If the answer is yes, then the employer is vicariously liable even though the work is being carried out in an unauthorised or improper manner.[515] However, an employer is not vicariously liable for independent wrongful acts of employers.[516] A breach of an express prohibition by the employee will not automatically place the employee outside the course of employment.[517] It will only have that effect if the nature of the prohibition is beyond the employee's role as described by the employer, rather than of the manner in which it is to be performed.[518]

An employer may be able to absolve itself from liability if it can be established that the action of the employee is "not reasonably incidental" to their duties.[519] The fact that the employee knows that the tortious act is a deliberate breach of the contract of employment is irrelevant if the act has a connection with their employment.[520]

The most litigated issue in recent times in tort claims concerning vicarious liability has been the issue of whether deliberate, possibly criminal, conduct may fall within the "course of employment", such as in the matter of Punchard. The traditional approach has been to identify whether the employee's conduct was an authorised act (clearly within), an improper, even a prohibited, mode of committing an authorised act (still within) or, on the other hand, an entirely remote and disconnected act, a "frolic of his own" as if a stranger to the employer (outside). This approach has proven unhelpful when considering certain examples of intentional, criminal behaviour.

---

510 Ibid 7.

511 Ibid 16.

512 Ibid [13].

513 Richards Ludlow Gibson, Tort Law in Principle 5th Edition (Thomson Reuters (Professional) Australia Limited, 2009) 387, quoting La Forest J in London Drugs Ltd v Kuehne International Ltd [1992] 3 SCR 299.

514 Richards Ludlow Gibson, Tort Law in Principle 5th Edition (Thomson Reuters (Professional) Australia Limited, 2009) 392.

515 Commonwealth v Connell (1986) 5 NSWLR 218.

516 Owston v Bank of New South Wales (1879) 4 App Cas 270.

517 Century Insurance Co Ltd v Northern Ireland Transport Board [1942] AC 509.

518 Richards Ludlow Gibson, Tort Law in Principle 5th Edition (Thomson Reuters (Professional) Australia Limited, 2009) 392.

519 Ibid 393.

520 General Engineering Services Ltd v Kingston [1988] 3 All ER 867.

The High Court of Australia [in *Prince Alfred College Inc v ADC* [2016] HCA 37 (*Prince Alfred College* 2016)], taking a slightly different approach, requires the court to look at whether the employee was placed in a position of power and intimacy, and whether the employer provided not merely the opportunity for the tort to be committed, but also the "occasion" for the tort. The possible extension of agencies' liability for public officers' conduct at work to cover their criminal offences was confirmed by Professor McDonald during her evidence, when asked if the *Prince Alfred College* 2016 judgment extended agencies' liability to cover criminal offences:

> *Well I think it's arguable.*

Therefore, there exists recent authority from the High Court to support the proposition that an employer is liable for the criminal actions of its employees undertaken at work, including misuse of confidential information.

Chapter 12 — Privacy by Design and best practice

The purpose of this chapter is to provide agencies with a guide on how to imbed privacy into their day-to-day work in the performance of their functions. Privacy should not be an afterthought or considered as a compliance obligation with minimum standards to reach. Rather privacy needs to be a part of the every day. Earlier in this report it discussed the steps that agencies can take to mitigate the corruption risks which relate to misuse of confidential information. At the heart of this is the need to change organisational culture — a positive approach to privacy will only get authentic traction if thinking about "privacy first" becomes the norm.

Privacy by Design (PbD) is an approach that was developed to assist decision-making processes, and foster a privacy-conscious organisational culture in public and private sector entities. PbD ensures that privacy is considered at the outset of any venture, and additionally at important points in time throughout the venture's duration, to ensure privacy is incorporated into the initiative's design as it evolves. This approach was first conceptualised in Canada in the 1990s by the former Privacy and Information Commissioner of Ontario.

PbD has since been used in the public and private spheres globally and is partially reflected in IPP4[521] [Storage and security of personal information]. IPP4 requires agencies that have control of a document containing personal information to ensure it is protected against loss, unauthorised access, use, modification or disclosure and any other misuse, and to take all reasonable steps to prevent its unauthorised use or disclosure. Queensland public sector agencies that store confidential information are therefore required to take steps that are reasonable to protect that information. Despite this, only two agencies subject of this report noted that they consider PbD approaches with respect to privacy protection related initiatives. The relevant agency responses are outlined below, for consideration by other Queensland public sector agencies.

Overview of PbD and its applicability to the Queensland context

PbD is seen by many as the global standard by which to construct privacy protection, evident by the EU GDPR at Article 25 [Privacy by Design By Default] which conveys the key principles underlying the entire regulation. When read in conjunction with Article 32 [Security of processing], commentary of the GDPR provides:[522]

> *Data privacy by design ensures that privacy is built into products, services, application, business and technical processes. Data privacy by default protects a natural person's fundamental rights and freedom to protection of their personal data.*

PbD should complement compliance requirements and should not be treated as a compliance obligation in and of itself. PbD initiatives ought to be integrated into a revised "contemporary legislative framework to manage new and emerging privacy risks" as submitted in the OIC's 2017 submission to DJAG[523]. The new contemporary framework would see the creation of a mandatory NDB scheme in Queensland, and the OIC having own-motion powers and scope to issue a post own-motion investigation declaration. The CCC is supportive of these submissions.

The OAIC's *Guide to securing personal information* (the OAIC Guide) was developed to give entities guidance on PbD approaches to protecting confidential information from misuse. Although this

521 IPA.

522 'GDPR Article 25', Imperva (2019), < https://www.imperva.com/learn/data-security/gdpr-article-25/>.

523 '*2016 Consultation on the Review of the Right to Information Act 2009 and the Information Privacy Act 2009*' (2017), p. 50.

document is not legally binding and despite it being intended for use by entities covered by the Privacy Act rather than the State's comparable Act (namely, the IP Act), the CCC nevertheless considers it an authoritative and useful guide in the Queensland context. The recommendations contained throughout this report embody a generality that the Queensland privacy regime ought to be adapted to reflect more consistently the Commonwealth's privacy architecture. Given this, the OAIC's Guide discussed below is recommended for reference by public sector agencies in Queensland until such time as there is a Queensland counterpart guide and in lieu of the recommended legislative and policy changes.

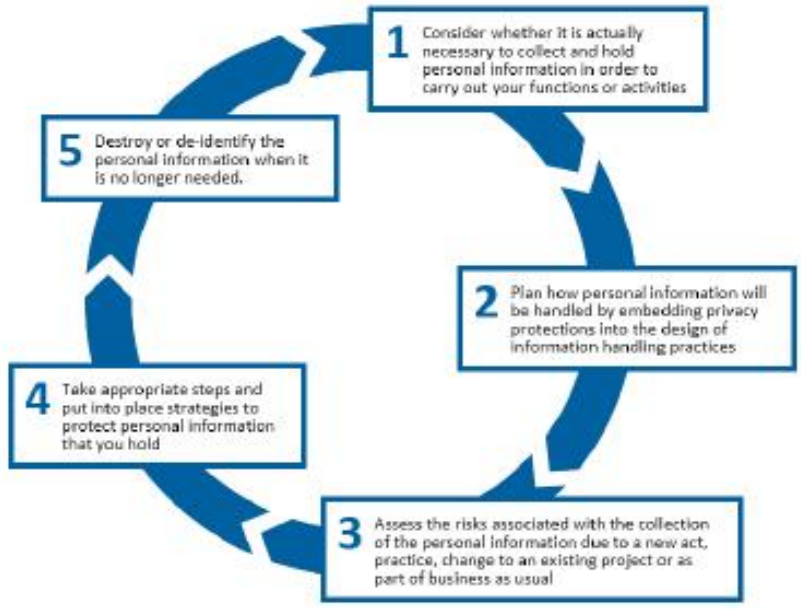
The OAIC Guide

The OAIC Guide[524] recommends that an entity's measures to protect confidential information should aim to:[525]

- Prevent the misuse, interference, loss or unauthorised accessing, modification or disclosure of personal information;
- Detect privacy breaches promptly; and
- Be ready to respond to potential privacy breaches in a timely and appropriate manner.

Agencies are advised to determine reasonable steps not just at the outset of a project, but throughout the "information lifecycle" of a given initiative.[526]

Figure 3: The information lifecycle



Source: OAIC Guide, p. 8.

Figure 3 shows the process of safeguarding confidential information as a lifecycle, which is broken down into five distinct stages. This approach requires agencies to consider when and how information is being collected, and when and how it is being stored.[527]

524 OAIC (2018) Guide to securing personal information: "Reasonable steps" to protect personal information

525 Ibid p. 9.

526 Ibid, p. 7.

527 Ibid.

The OAIC recommends that an organisation will be better equipped to appropriately access, manage and store confidential information if associated principles are embedded and entrenched early, revisited and refreshed where needed throughout the information lifecycle.

Privacy Impact Assessments (PIA)

When assessing risks, the OAIC Guide recommends that agencies conduct a privacy impact assessment (PIA). Once an entity collects and holds confidential information, consideration of appropriate security measures is required to protect and manage that information. Different types of information may attract different levels of associated risks, which may require an entity to afford different security measures to adequately protect that category of information.[528]

A PIA is a mechanism to expedite maturity of an agency's integration of PbD principles. PIAs are designed to help agencies identify privacy impacts that might arise in response to a given project or proposal, and generates ways to manage, reduce or rid of those impacts. Conducted at an early stage of a project, a PIA can influence the design of the project and identify reasonable steps that should be taken by an agency to protect personal information.[529]

A PIA should comprise the following attributes:

- Description of the ways personal information will flow into the possession of the agency;
- Analysis of the possible privacy impacts of the above-stated flows;
- Assessment of the impact the project in its entirety might have on individuals' privacy; and
- Explanation of how those impacts will be reduced or eliminated.[530]

As a general rule, as the volume and or the sensitivity of confidential information stored by an entity increases, so too should the steps to protect it increase and augment to suit that entity's needs. The size and complexity of an entity will also impact on the steps considered reasonable to protect that entity's repository of confidential information. This is reflected in privacy legislation, which dictates that sensitive information attract a greater level of protection than non-sensitive information. In any event, entities are not excused from taking steps to protect personal information due to the exercise being inconvenient, time-consuming or costly.[531]

PIAs are featured in the OIC's report *10 Years On—Queensland government agencies' self-assessment of their compliance with the Right to Information Act 2009 (Qld) and the Information Privacy Act 2009 (Qld)* (the 10 Years On Report), which reviewed the RTI and IPA 10 years after their commencement in July 2009. The report advised agencies to "build privacy protections into the design of…emerging technologies [and]… build privacy impact assessments into all project design and management frameworks".[532] The report also found: [533]

> *Reassessing the privacy impacts of the system or process after it is in operation, for example when updates are deployed or new features are released, will help ensure that the agency continues to approach privacy as a "design feature" of its processes and activities.*

528 Ibid, pp. 11, 14.

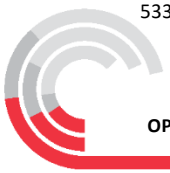
529 Ibid, p. 9-10.

530 ibid, p. 10.

531 Ibid, 12-15.

532 Ibid.

533 Ibid, p. 30.



The 10 Years On Report was supportive of PIAs being:[534]

> *…core business and that all agencies must protect personal information…Project management methodologies and tools should include privacy impact assessments as key deliverables during design, development and operation of all agency functions. This is core business for any agency when it is managing personal information.*

The Privacy Commissioner, Philip Green, during his evidence spoke of the importance of conducting ongoing PIAs, during the design phase of a given initiative and at regular intervals thereafter to assess ongoing, evolving and/or new threats. Mr Green explained that PIAs:—

> *…look at the whole picture…look at all of the data flows, look at all of the risks and then put mitigation strategies in place to deal with the risks.*

Current use of PIAs in Queensland

During the public hearing, DTMR gave evidence about its use of PIAs. Director-General Neil Scales said during his evidence that PIAs are being used with respect to "all new programs and projects". In consultation with the OIC, Mr Scales told the CCC that: [535]

> *…we* [the DTMR] *are heading in the right direction, with the right security protocols, the right access controls…we have got an Information Security Unit who will conduct penetration and testing and also security risk assessments…we actually bring the [relevant] agencies in right at the start of any new project…so they can add value on all the way through.*

The Privacy Commissioner, Philip Green, having regard to DTMR's Translink and TRAILS databases, said that risk-based, principled approaches are "very good for the reasonableness test" and are "very, very healthy and a far greater step along maturity".[536]

An important element of PbD is to integrate privacy into risk-management processes in order to fully embed good practices for handling confidential information, which will assist with effective response in the event of a privacy breach.[537]

Reference to and assistance from the OAIC Guide

This part outlines salient features of the OAIC Guide to assist public sector agencies determine "reasonable steps". This part has been referred to in other chapters of this report as best practice guidance for Queensland public sector agencies despite its applicability to Commonwealth privacy legislation. It is advisable that public sector agencies have regard to the OAIC's Guide in conjunction with this report for further detail and discussion of the following points raised.

The OAIC outlined the following circumstances that might impact on an agencies' categorisation of a reasonable step to ensure the security of personal information in its possession:[538]—

- The nature of the entity;
- The amount and sensitivity of the personal information held;
- The possible adverse consequences for an individual in the case of a breach;
- The practical implications of implementing the security measure, including the time and cost involved; and

534 Ibid, p. 31.

535 Evidence given by Neil Scales on 11 November 2019, p. 20-21.

536 Evidence given by Philip Green on 22 November 2019, p. 15.

537 OAIC (2018), *Guide to securing personal information, "reasonable steps" to protect personal information*, p. 9.

538 Ibid, p. 12.

- Whether a security measure is itself privacy invasive.

These circumstances and surrounding commentary are discussed in more detail above in this report. However, at this point it is important to highlight that even slight variations of a factual scenario may lead to different "reasonable steps" to be taken.

Steps and strategies that may be reasonable to take

The following is a list of practical steps and strategies categorised under nine broad topics to assist agencies protect confidential information. The nine broad topics are listed as follows:[539]

1. Governance, culture and training;
2. Internal practices, procedures and systems;
3. ICT security;
4. Access security;
5. Third party providers (including cloud computing)
6. Data breaches;
7. Physical security;
8. Destruction and de-identification; and
9. Standards.

The above-listed broad topic categories are not an exhaustive list and regard ought to be had by agencies to relevant standards and guidance on information security.[540] Outlined below is a brief discussion of each step/strategy to assist agencies' understanding of what may constitute a reasonable step.

1. Governance, culture and training

Fostering a privacy and security aware culture

Personal information security should form an integral part of an agency's core business and not be reserved for compliance or ICT areas in isolation. A privacy and security conscious management focus is needed to foster a privacy and security aware organisational culture. Privacy and security governance arrangements should be reflected and built-in to staff training material, and made available via the adequate allocation of resources. This will ensure that appropriate approaches to ensuring personal information security will permeate an organisation throughout its entire business, but only with the active support and promotion by senior management.[541]

Oversight, accountability and decision-making

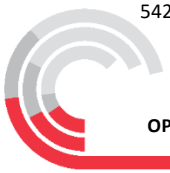
The OAIC's Guide542 suggests designating a group or individuals with responsibility for having up-to-date knowledge of the personal information held by their given agency as a way of ensuring that it is held securely. This is suggested as being complementary to having clear procedures in place in relation to oversight, accountability and decision-making channels of authority. It is envisaged these

539 Ibid, p. 16.

540 OAIC (2018) Guide to securing personal information, "reasonable steps" to protect personal information, pp. 16-42.

541 Ibid, p. 17.

542 OAIC (2018) Guide to securing personal information, "reasonable steps" to protect personal information, p. 17.



individuals or internal body could be responsible for defining, implementing and managing information security measures, for review by senior management.[543]

For example, the designated team or group of individuals dispersed through an agency may look into and determine whether appropriate procedures are in place regarding the agency's ability to respond efficiently to privacy breaches.

Personnel security and training

Personal information security includes ensuring that staff are aware of and understand their responsibilities and obligations as regards privacy, good information handling and security practises. Training to that end is to be undertaken by all staff including management, new starters, contractors and temporary staff.[544]

2. Internal practices, procedures and systems

The OAIC's Guide stipulates that reasonable steps are required to be taken by agencies to develop and maintain practices, procedures and systems to ensure compliance with the APPs and any related registered APP code. APP codes once registered operate in addition to the APPs, a breach of which will be an interference with the privacy of an individual by the entity.[545]

With respect to APP 11 in particular, the OAIC recommends that internal practises, procedures and systems used to protect personal information be documented by agencies and made accessible to all staff. Decisions relating to security choices made by agencies should also be recorded, including reasons for those approaches.[546]

Consistency of language becomes necessary to highlight at this point. Ensuring language has applicability across an entire business unit, having regard to consistency with relevant privacy laws, is critical to ensuring that all staff understand their obligations under the relevant regulatory regimes.

3. ICT security

Effective ICT security necessitates that an agency's hardware and software are protected from misuse, interference with, loss, unauthorised access to, modification and/or disclosure without inhibiting the ability of authorised users to use systems efficiently for legitimate work related purposes.

Regular monitoring is required to ensure ICT security measures are responsive to changing and dynamic threats. Consideration of any potential system vulnerabilities that might impact on staff, persons or systems that interact with the subject ICT system is required to mitigate risks of internal or external unauthorised accesses.

Software security, encryption, network security, whitelisting and blacklisting, testing, backing up and email security are ICT security measures discussed in the OAIC's Guide[547] as a guide for agencies determining reasonable steps under this category.

4. Access security

The OAIC recommends that agencies proactively protect themselves against internal and external risks through the development of access security and monitoring controls. Such measures will help

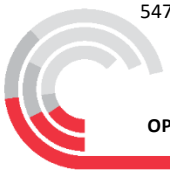
543 OAIC (2018) Guide to securing personal information, "reasonable steps" to protect personal information, p. 17.

544 Ibid, p. 18-19.

545 'Office of the Australian Information Commissioner – APP Guidelines', Version 1.3, July 2019, p. 25 [B.123-125].

546 Ibid, p. 20-21.

547 OAIC (2018), Guide to securing personal information, "reasonable steps" to protect personal information, p.23-28.



ensure that only authorised persons access personal information available on a given agency's database.

Access security initiatives are to incorporate "unauthorised access" and "disclosure" as separate concepts; both may result in a breach of privacy principles if the agency did not take reasonable steps to protect personal information.[548]

Trusted insider risk

This sub section is of particular relevance to Operation Impala. It requires that agencies be alive to possible internal incidences of unauthorised access or misuse of personal information by staff (including contractors).[549]

The OAIC recommends that internal access to personal information should be limited to minimise the trusted insider risk, namely to provide access on a need-to-know basis as an important personal information security mechanism.[550]

Audit logs, audit trails and monitoring access

Maintaining a chronological system activities record, such as an audit log, is noted by the OAIC as often being the "best way" to review, detect and investigate privacy incidences.[551]

Further, efforts to identify potential misuses of personal information or anomalous behaviour, including work in furtherance of proactive monitoring, may be a reasonable step particularly in instances where an agency holds a large volume of personal information.[552]

Example practical application

Having regard to the "trusted insider risk" and "audit logs, audit trails and monitoring access" sub categories of "4. Access security", auditing databases that store personal information may assist agencies protect itself against internal data breach incidences.

The application of the above-stated sub categories is outlined below, which may be helpful for agencies when determining what reasonable steps it should take to protect personal information it holds. This exercise also highlights deficiencies with the implementation of information security strategies despite worthy objectives

Commissioner of Police, QPS

Evidence given by Katarina Carroll, Commissioner of Police, on 18 November 2019 confirmed that QPRIME is a fully auditable system, every access is logged and kept for 80 years.[553] Despite this, the QPS had earlier confirmed in their response to a CCC request for information that:[554]—

> *QPRIME does not specifically restrict or categorise records relating to vulnerable or high profile persons. This reflects the nature of policing and prevalence of dealing with people who may fall within the vulnerable categorisation…The option is*

548 'Office of the Australian Information Commissioner – APP Guidelines', Version 1.3, July 2019, Chapter 11, p. 6.

549 OAIC (2018) Guide to securing personal information, "reasonable steps" to protect personal information, p. 28.

550 Ibid.

551 OAIC (2018) Guide to securing personal information, "reasonable steps" to protect personal information, p. 32.

552 Ibid.

553 Evidence given by Katarina Carroll on 18 November 2019, p. 18.

554 Exhibit 97 of CCC Operation Impala public hearings.

exercised on a case by case basis and in certain circumstances such as records relating to covert identities and operations.

Moving forward, the Commissioner acknowledged the following areas for improvement:

- That vulnerable persons categories be developed, including a category for persons in domestic and family violence situations (following the evidence of Professor Barbara McDonald)[555];
- Put flags or alerts on prominent database entities, including domestic violence victims or high profile persons;[556] and
- That regular audits be conducted having regard sensitive information, in addition fiscal issues and resource considerations.

It was highlighted during the Commissioner's evidence that these initiatives would need to be balanced by operational needs of police officers. Counsel Assisting noted the approach of Tasmanian police insofar as it not being common practice that police officers' access rights are restricted.[557] These proposals are detailed above in this report.

Director-General, Department of Health

- Health information, in and of itself, is more sensitive than other information. Steps taken by agencies to protect that information therefore are to be tailored to accord to the increased level of risk associated with that information as confirmed by Director-General of the Department of Health during his hearings evidence[558]. This is also legislatively reflected by the delineation of the IPPs and the NPPs, the latter creating a separate regime for "sensitive information" (that includes 'health information') which provides specific provision for appropriate ways of handling health information in specified circumstances.[559]
- Exhibited in evidence was a departmental response from DoH which conveyed a current strategic focus as being "adopting a more positive Privacy by Design approach, particularly in the establishment phase of new systems/projects/programs".[560] By extension, PbD approaches ought to have been incorporated into the introduction and roll-out of the P2Sentinel software project used by HHSs to monitor and detect potential data breaches of the new ieMR database. A challenging area for the Department of Health thereby arising, and discussed with witnesses from the Mackay and Gold Coast HHSs, is working through the backlog of potential data breaches generated as a result of this otherwise positive initiative.
- To date, DoH has not taken steps to rectify the HHS backlog. However, the Director-General of DoH, Dr John Wakefield during his hearings evidence agreed there may be scope for it to collaborate with, and provide assistance to, HHSs to manage the backlogs and progress related reporting obligations thereby arising, as detailed above in this report.[561]

555 Evidence given by Barbara McDonald on 15 November 2019, p. 22.

556 Noted in the 'Report of an own-motion investigation into the management of information in Tasmania Police', Report of the Integrity Commission, No. 3 of 2018, p. 34 [151]; and the Independent Broad-based Anti-corruption Commission Victoria report, 'Unauthorised access and disclosure of information held by Victoria Police: an analysis of corruption risks and prevention opportunities', September 2019, p. 21.

557 Report of an own-motion investigation into the management of information in Tasmania Police', Report of the Integrity Commission, No. 3 of 2018, p. 34 [155].

558 Evidence given by Dr John Wakefield on 14 November 2019, p. 40.

559 Australian Law Reform Commission Report 108 'For Your Information: Australian Privacy Law and Practice' (the 2008 ALRC Report)

560 Department of Health response to CCC questions on 21 and 22 October 2019, Exhibit 68.

561 Evidence given by Dr John Wakefield on 14 November 2019, p. 28.

Ways to prevent and approach risks associated with identity management and authentication, collaboration, access to non-public content, passwords and passphrases, and individuals accessing and correcting their own personal information are outlined in more detail on pages 29 to 34 of the OAIC's Guide.

5. Third party providers (including cloud computing)

Personal information handling may be outsourced by some entities to third party providers, which extends to data storage services by cloud-based service providers. Determination of whether that entity still 'holds' that information is firstly needed[562], then consideration as to whether the third party provider has obligations arising under the relevant privacy legislation. If the entity that outsourced the information handling is determined to still "hold" the personal information[563]—that is, if the entity has possession or control of a record containing personal information—that entity is still required to consider what steps are reasonable to protect the personal information even if the third party provider is also subject to the relevant Act.[564]

6. Data breaches

Agencies should have a response plan in the event of a data breach. Procedures and a clear articulation of lines of authority should be included in a response plan to assist with containment and management of the breach.

It is important to ensure staff, including contractors, are aware of and understand the response plan and imperative of reporting breaches—the OAIC notes this as being essential for the effectiveness of the plan.[565]

7. Physical security

Agencies are to consider steps that might be necessary to ensure physical copies of personal information are secure. Some examples of physical security measures include security and alarm systems used to control entry to a workplace, access logs kept to monitor staff entering and leaving the workplace, a record management system to track the location of files, a clean desk policy and its enforcement, a procedure for working on sensitive matters at off-site locations, and the availability of lockable cabinets or similar to store personal information.[566]

8. Destruction or de-identification of personal information

If there is no longer a need to hold personal information, the relevant entity holding that information must ensure it takes steps that are reasonable to destroy or de-identify it, or take another step that is reasonable in the circumstances. It is important to have regard to any obligations arising under other laws, or court or tribunal orders, in addition to retention obligations that attach to personal information contained in a Commonwealth record under the *Archives Act 1983* (Cth).[567]

Irretrievable destruction of personal information includes destruction of hard and electronic forms of personal information, and extends to destruction of copies stored on a third party's hardware (in cloud storage) and in other back-up technologies used by the agency. Putting personal information held in electronic form "beyond use" is distinct from irretrievable destruction. This might occur when it is not possible for an agency to irretrievably destroy personal information kept electronically; for

562 Having regard to APP 11—security of personal information.

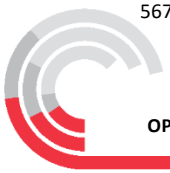
563 Privacy Act 1998 (Cth), s 6 & 10.

564 OAIC (2018) Guide to securing personal information, "reasonable steps" to protect personal information, p. 34.

565 Ibid, p. 37.

566 OAIC (2018) Guide to securing personal information, "reasonable steps" to protect personal information, pp. 38-39.

567 Ibid, p. 39.



example, circumstances might exist wherein irretrievable destruction of personal information would simultaneously destroy other personal information required to be held with it[568].

De-identification of personal information might be more appropriate in the circumstances than destruction. "De-identified" personal information is just that if it is no longer about an identifiable individual or an individual who is reasonably identifiable.[569]

Agencies are to consider what kind of destruction or de-identification of personal information is reasonable in the circumstances.

9. Standards

The OAIC Guide recommends entities use relevant standards for guidance on information security. Standards may include guidelines, handbooks, policies or manuals designed to give clarity on the way products, services or systems should be used or performed.

Of note, while adopting a standard may help an agency gain confidence regarding their security practices, it does not avail it from taking (additional) steps that are reasonable to protect personal information. Further, application of what "personal information" and "sensitive information" means under privacy law is required even if there has been adoption of a standard—this is necessary in order to meet security requirements required under the privacy principles.[570]

Additionally, agencies are encouraged to consult the internationally recognised ISO IEC 27001:2013 Information Security Management System standard, some of which has been adopted by Standards Australia. QGCIO has had an information security policy for over 10 years, which was recently upgraded to align with international standards. The new policy, entitled IS18:2018, has three requirements. Agencies must apply a systematic and repeatable approach to risk management, meet the minimum security requirements, and attest to the appropriateness of the agency's information security.[571]

Establishment of an executive level "information privacy champion"

Chief Privacy Officer (CPO) example

The CCC also examined[572] privacy initiatives used by other jurisdictions that that could be of potential benefit to Queensland. The New Zealand CPO is wholly responsible and accountable for keeping privacy considerations at the forefront across government, through the development and dissemination of related expectations and guidance. The CPO core function explained generally is to help facilitate good practice, learning from those entities doing well to assist others to mature their privacy position. A key part of the CPO's daily role is to personally interact with privacy officers working at an operational level and agency executives to discuss how projects are progressing, the challenges agencies are confronting, and workshopping ideas to address those difficulties in a way that is privacy conscious.

568 Ibid, p. 39.

569 s. 6 [Interpretation] of the *Privacy Act 1988* (Cth).

570 OAIC (2018) Guide to securing personal information, "reasonable steps" to protect personal information, pp. 41-42.

571 Evidence given by Andrew Mills on 20 November 2019, pp. 5-6.

572 Nicole Stephensen, Principal Consultant at Groundup Consulting was consulted by the CCC to provide practical insight into the development of privacy legislation in Queensland, particular due to her experience providing drafting instruction regarding the IPA and her role in the whole-of-government implementation of the state's previous administrative privacy regime.

The CPO's four main functions comprise: 1) the provision of leadership; 2) building capability; 3) providing advice and assurance; and 4) engaging with the regulator and citizens.[573]

The CPO is not a regulator but is described as being more akin to a coach providing assistance and resources to agencies regarding an all-of-government view of privacy. The role was created in 2014 following a raft of privacy-related incidents that reduced public trust in government's capacity to handle the member of the public's personal information. The CPO reports annually to the relevant Minister as regards privacy maturity across the sector. In its second publicly available annual report published in 2017, the CPO reported there to have been "collective improvement overall in both privacy and protective security capability since the 2016 reporting round".[574] Although agencies were reported as having made steady progress in building privacy and protective security capabilities, the CPO recommended that complementary cross-government imperatives were needed to entrench and accelerate the prioritisation of privacy.[575]

Suitability for Queensland

It is acknowledged that privacy officer roles presently operate in Queensland public sector agencies. Although some privacy considerations are devolved to them, the scope of their work usually consists of responding to RTI requests. As a result, persons in these positions are usually stifled in their ability to be a champion for privacy, being unable to advocate for PbD into workplace initiatives, given the sheer volume of operational requests to be actioned.

Privacy officers therefore currently lack the standing required to make privacy-oriented, strategic recommendations to executive level agency staff. For this reason the CCC supports the creation of a "privacy champion" role to be taken up by a senior officer of a public sector agency.

Depending on a range of factors including the size of the agency, the nature and volume of the confidential information in its possession, the CCC suggests that a stand-alone senior officer position be created to perform this function. As an alternative, the CCC recommends representation at the executive level—that is, that a member of the agency's executive be given responsibility to advocate for privacy during strategic decision-making processes.

Recommendation 18 – Privacy Champion

That a "privacy champion" be embedded in agencies at a senior officer level, with the view to incorporating PbD into executive decision-making processes.

573 'Focusing the Department of Internal Affairs' delivery of its government ICT functional leadership and information management mandate', Cabinet State Sector Reform and Expenditure Committee, Office of the Minister of State Services (2017), p. 5.

574 'Annual report to Minister of State Services on privacy and protective security', (June 2017), New Zealand Security and Intelligence Service, The Department of Internal Affairs, p. 1.

575 Ibid, pp. 6-8.

Chapter 13 — Conclusion

Based on the findings of Operation Impala, the CCC's assessment is that public sector agencies are at varying levels of maturity in their approaches to dealing with confidential information. It found that individual agency approaches and degree of risk awareness were generally influenced by:

- the types of information they collect and manage, and
- how strongly organisational culture reinforces the importance of protecting confidential information.

As observed at the beginning of this report, there has been a general increase in the number of allegations of misuse of confidential information across the public sector, although there may still be significant under-reporting. The CCC considers that the higher number of allegations reflects an increasing maturity in agencies, demonstrated by their readiness to take more proactive steps towards detection, recognition and reporting of misuse of confidential information.

The CCC hopes that agencies will adopt the recommendations made in this report. They have been designed to strengthen public sector information management systems and to build greater awareness of the need to protect confidential information. A framework of auditable access controls, supported by clear policies and procedures and reinforced by training and communication from management, will build an effective privacy culture that the Queensland community can have confidence in. The community should also be able to trust that those employees who are found to have improperly accessed or misused confidential information will be sanctioned promptly, appropriately and consistently, regardless of the agency they work for.

Finally, it has been a prime concern of the CCC and of the many other parties who contributed to Operation Impala that the victims of privacy breaches — particularly the most vulnerable — should, in future, find it less difficult to have their situation acknowledged and, if appropriate, compensated. To this end, it hopes that its recommendations reflect that their concerns have been heard and will be addressed.

Appendix 1 — Terms of reference

Context

The Queensland Crime and Corruption Commission (CCC) has received a number of allegations of corrupt conduct within Queensland public sector agencies, relating to misuse of information. The allegations include both improper access to, and improper disclosure of, confidential information.

Historically, the Queensland Police Service (QPS) has attracted the most complaints in this area. Since 2016 the QPS and the CCC have worked to educate and deter officers and staff of the QPS on this corruption risk area. There has been a decrease in the number of complaints within QPS over this period of time. Meanwhile, the number of allegations has been increasing in other areas of the public sector, and it is reasonable to also suspect a level of non-reporting in the sector.

In discharging its corruption function, the CCC has conducted investigations of alleged corrupt conduct relating to misuse of information within the Queensland public sector, both directly, and in its monitoring role. As a result of investigations conducted, a number of possible systemic issues have been identified. This project will examine these issues with a view to raising standards of integrity relevant to: detecting, managing and preventing corruption risks associated with misuse of information within the public sector; and the way allegations of suspected corrupt conduct against public sector staff are dealt with by the various agencies.

Objectives of the Public Hearing Component of Operation Impala

Pursuant to sections 176 and 177(2) (c)(ii) of the *Crime and Corruption Act 2001*, the Commission authorises and approves the holding of public hearings in relation to the misuse of information.

The CCC public hearing is examining:

1. Factors which facilitate misuse of information within the Queensland public sector, by examination of the technical, people, and systems components of information management within the following identified agencies – Queensland Police Service, Queensland Corrective Services, Department of Education, Department of Health (including selected Hospital and Health Services) and Department of Transport and Main Roads.
2. Features of the legislative, policy and operational environment within each agency that may enable corrupt conduct to occur or are vulnerable to corrupt conduct.
3. Reforms to better prevent, detect and deal with corrupt conduct relating to misuse of information within the identified agencies, and lessons that can be extrapolated to the broader Queensland public sector.

Public Report

The CCC will issue a public report on the outcomes of this project.

Appendix 2 — List of witnesses at the public hearing

11 November 2019

Peter Martin APM, Commissioner, Queensland Corrective Services

Dr Russell Smith, Principal Criminologist, Australian Institute of Criminology

Neil Scales, Director-General, Department of Transport and Main Roads

Sandra Slater, Chief Information Officer, Department of Transport and Main Roads

12 November 2019

Tony Cook PSM, Director-General, Department of Education

David Miller, Executive Director, Integrity and Employee Relations, Department of Education

Rod Francisco, Executive Director, People, Mackay Hospital and Health Service

Edmund Burke, Representative for Queensland Teachers' Union of Employees

13 November 2019

Marty Mickelson APM, A/Assistant Commissioner, Office of State Discipline

Hannah Bloch, Executive Director, People and Corporate Services, Gold Coast Hospital and Health Service

14 November 2019

Dr John Wakefield, Director-General, Queensland Health

Damian Green, Chief Executive Officer, eHealth Queensland

Sandra Eales, Assistant Secretary, Queensland Nurses and Midwives Union

15 November 2019

Professor Barbara McDonald

James Koulouris, Deputy Commissioner, Queensland Corrective Services

Kim Papalia, Assistant Commissioner, Professional Standards and Governance Command, Queensland Corrective Services

Matthew Bell, Senior Sergeant, Security Incident Registry, Victoria Police

18 November 2019

Katarina Carroll APM, Commissioner, Queensland Police Service

Sharon Cowden APM, Assistant Commissioner, Queensland Police Service Ethical Standards Command

Ian Leavers, President, Queensland Police Union of Employees

19 November 2019

Sarala M C Fitzgerald

Renee Eaves

Timothy Joseph Dillon, A/ Director Digital Transformation and End User Tools & Platforms, Public Safety Business Agency

Rosemary O'Malley, Chief Executive Officer, Domestic Violence Prevention Centre

20 November 2019

Matthew Vanderbyl, Chief Superintendent, Organisational Capability Command, Queensland Police Service

Andrew Mills, Queensland Government Chief Information Officer

Geoffrey Magoffin, Customer Service General Manager

22 November 2019

Professor Geraldine Mackenzie

Scott McDougall, Commissioner, Queensland Human Rights Commission

Philip Green, Privacy Commissioner, Office of the Information Commissioner

Rachael Rangihaeata, Information Commissioner, Office of the Information Commissioner

Appendix 3 — DTMR information campaign poster

Department of Transport and Main Roads

When it comes to information privacy, a peek is a breach!

We all have an obligation to make sure our customers' personal information remains safe and secure.

Unauthorised access of someone else's personal information is a very serious matter. Even a simple peek is a breach of the TMR Code of Conduct and is an unlawful invasion of privacy.

The consequences for this kind of behaviour can go beyond disciplinary action from TMR.

It may also:

- result in a criminal conviction
- impact on the customer's circumstance and safety
- damage your own and TMR's reputation
- result in TMR being prosecuted.

We have an obligation to report breaches to those affected. We monitor and record system activity, so if you do the wrong thing you will be caught.

Don't risk it!

More information

Refer to CSB's Accessing Customer Records policy on InsideCSB for more information or talk to your manager.

Queensland Government

References

Ankamah, S. S., & Manzoor E Khoda, S. M. (2018). Political will and government anti-corruption efforts: What does the evidence say?. *Public Administration and Development*, 38(1), 3-14.

Australian Law reform Commission (ALRC) (2008). *For Your Information: Australian Privacy Law and Practice*, Report 108.

— (2014). *Serious Invasions of Privacy in the Digital Era*, Report 123.

— (2014). Discussion Paper: *Serious Invasions of Privacy in the Digital Era*, 30 March 2014.

Cherdantseva, Y., & Hilton, J. (2013). A reference model of information assurance & security. In 2013 *International Conference on Availability, Reliability and Security*, p. 552, IEEE.

Crime and Corruption Commission (2019). *Annual Report 2018-19*.

— (2018). *Taskforce Flaxton: An examination of corruption risks and corruption in Queensland prisons*.

— (2018). *Improper access to public sector databases: what you should know*. https://www.ccc.qld.gov.au/sites/default/files/Docs/Publications/CCC/Prevention-in-Focus-Improper-access-to-public-sector-databases-2018.pdf

— (2019). Improper access to public sector databases, no. 2. https://www.ccc.qld.gov.au/sites/default/files/Docs/Publications/CCC/Prevention-in-Focus-Improper-access-to-public-sector-databases-no2-2019.pdf

Criminal Code Advisory Working Group (Qld) (1996). Report of the Criminal Code Advisory Working Group to the Attorney-General.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, 20(1).

Da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security*, 49.

de Vries, Kevin. (2019). Privacy, confidentiality and health information. *Australian Journal of Pharmacy*, May 2019. https://ajp.com.au/cpd-activities/privacy-confidentiality-and-health-information/

Department of Education (2019). *Annual Report 2018-2019*. https://qed.qld.gov.au/det-publications/reports/Documents/annual-report/18-19/annual-report-2018-19.pdf

Department of Justice and Attorney-General (2017). *Review of the Right to Information Act 2009* and the *Information Privacy Act 2009*

DSITIA (2013). Queensland Government ICT strategy 2013-2017 action plan, p. 20. https://s11217.pcdn.co/wp-content/uploads/2013/08/ict-strategy-action-plan.pdf

Hutchings, A., & Jorna, P. (2015). Misuse of information and communications technology within the public sector, p. 1. Accessed from https://aic.gov.au/publications/tandi/tandi470

Independent Broad-Based Anti-Corruption Commission (IBAC) (2020). Recruitment and Employment. Accessed from https://www.ibac.vic.gov.au/preventing-corruption/are-you-vulnerable-to-corruption/recruitment-and-employment.

— (2019). *Unauthorised access and disclosure of information held by Victoria Police: An analysis of corruption risks and prevention opportunities*. Accessed from https://www.ibac.vic.gov.au/publications-and-resources/article/unauthorised-access-and-disclosure-of-information-held-by-victoria-police

— (2017). *Perceptions of corruption: Survey of Victorian Police employees*. https://www.ibac.vic.gov.au/docs/default-source/research-documents/perceptions-of-corruption-victoria-police.pdf?sfvrsn=482f7075_7

Integrity Commission (Tasmania) (2018). *Report of an own-motion investigation into the management of information in Tasmania Police*, Report of the Integrity Commission, No. 3 of 2018, p. 34 [151].

IPPA WA (2016). Information integrity pathway / roadmap for reform. http://www.wa.ipaa.org.au/content/docs/2016/Research-Day/Papers/S3.1_Do_government_organisations.pdf

ISO/IEC 27001:2015. Information technology – security techniques – information security management systems – requirements.

Kuo, K. M., Talley, P. C., Hung, M. C., & Chen, Y. L. (2017). A deterrence approach to regulate nurses' compliance with electronic medical records privacy policy. *Journal of medical systems*, 41(12)

Lynch, C (2019). Cop charged with hacking police system in south-east Queensland, *Brisbane Times*, 16 July 2019. https://www.brisbanetimes.com.au/national/queensland/cop-charged-with-hacking-police-system-in-south-east-queensland-20190716-p527t7.html

Mckenzie, N., Baker, R., Silvester, J., & Houston, C. (2016). Nightclubs, dirty cops, drugs and leaks: the inside story. *The Age*, 23 September 2016. https://www.theage.com.au/national/victoria/nightclubs-dirty-cops-drugs-and-leaks-the-inside-story-20160923-grncbj.html

More, Georgie (2019). Ex-policeman jailed for passing data to private eye. *The Age*, 18 September 2019. https://www.theage.com.au/national/victoria/ex-policeman-jailed-for-passing-data-to-private-eye-20190918-p52ski.html

Office of the Australian Information Commissioner (OAIC) (2019) *Australian Privacy Principles guidelines*, Version 1.3, July 2019, p. 25 [B.123-125].

— (2019). *Notifiable Data Breaches Scheme 12-month Insights Report*. https://www.oaic.gov.au/assets/privacy/notifiable-data-breaches-scheme/statistics/ndb-scheme-12month-insights-report.pdf

— (2018). *Guide to securing personal information: "Reasonable steps" to protect information*.

— (2017) *Australian Community Attitudes to Privacy Survey*

— (2015). *Privacy management framework: enabling compliance and encouraging good practice*.

Office of the Information Commissioner (OIC) (Qld) (2019). *Information Management: Queensland government department maturity*. Report No.2, p. 1. https://www.oic.qld.gov.au/__data/assets/pdf_file/0008/38708/report-audit-of-information-management-maturity.pdf

— (2019) *10 Years On — Queensland government agencies' self-assessment of their compliance with the Right to Information Act 2009 (Qld) and the Information Privacy Act 2009 (Qld)*.

— (2018). *Awareness of privacy obligations: How three Queensland government agencies educate and train their employees about their privacy obligations.*

— (2017). 2016 Consultation on the Review of the Right to Information Act 2009 and the Information Privacy Act 2009'

Public Service Commission (PSC) (2010). *Code of Conduct for the Queensland Public Service*. https://www.forgov.qld.gov.au/code-conduct-queensland-public-service

Queensland Corrective Services (QCS) (2019*). Annual Report 2018-2019.* https://www.publications.qld.gov.au/dataset/qcs-annual-reports/resource/ac3ac1b4-6161-4859-a2e8-87e800c49331

— Custodial Operations Practice Directive, Daily Operations - Case Management. https://publications.qld.gov.au/dataset/qcs-procedures/resource/c39cafe1-5a7f-414d-9784-de111a668433

Queensland Government Chief Information Officer (QGCIO) (2018). *Information sharing authorising framework: Comprehensive guidance for information sharing*. https://www.qgcio.qld.gov.au/documents/information-sharing-authorising-framework

Queensland Police Service (QPS) *Annual Report 2018-2019*. https://www.police.qld.gov.au/sites/default/files/2019-09/FINAL%20QPS%20AR%202018-19.pdf

Rajakaruna, N., Henry, P. J., & Scott, A. J. (2019). Misuse of Police Information Systems: Predicting Perceived Likelihood of Misuse among Unsworn Police Employees. *Policing: A Journal of Policy and Practice*, Oxford University Press.

Richards Ludlow Gibson (2009). *Tort Law in Principle* (5th ed.). Thomson Reuters (Professional) Australia Ltd.

Siganto, J. & Burdo, M. (2015). The Privacy Commissioner and Own-Motion Investigations into Serious Data Breaches: A Case of Going Through the Motions? *UNSW Law Journal*, Vol 38(3), pp. 1145-1185.

Smith, R., Oberman, T., & Fuller, G (2018). *Understanding and responding to serious and organised crime involvement in public sector corruption*. https://aic.gov.au/publications/tandi/tandi534

TISN (2018). User-access management: A defence in depth control analysis. https://www.tisn.gov.au/Documents/User-Access+Management++A+Defence+in+Depth+Control+Analysis.doc

Victorian Auditor-General (2009). *Audit Summary of Maintaining the Integrity and Confidentiality of Personal Information*, 25 November 2009.

Crime and Corruption Commission

QUEENSLAND

Contact details

Crime and Corruption Commission
GPO Box 3123, Brisbane QLD 4001

Level 2, North Tower Green Square
515 St Pauls Terrace,
Fortitude Valley QLD 4006

07 3360 6060 or
Toll-free 1800 061 611
(in Queensland outside Brisbane)

07 3360 6333

More information

www.ccc.qld.gov.au

mailbox@ccc.qld.gov.au

@CCC_QLD

CrimeandCorruptionCommission

CCC email updates
www.ccc.qld.gov.au/subscribe