Crime and Corruption Commission
QUEENSLAND

February 2018

PREVENTION in focus

Improper access to public sector databases

What you should know

Officers who improperly access work databases can face dismissal or criminal prosecution

- Public sector agencies hold large amounts of private information about individuals — from their addresses and contact details to personal health information and information relating to contact with the police and the criminal justice system.
- Public agencies are obliged under the *Information Privacy Act 2009* to ensure that personal information is protected against unauthorised access, use, modification or disclosure. Improper access and use of such information, as well as potentially infringing on the privacy of individuals, can seriously compromise the effective carrying out of an agency's functions.
- Public agencies must have frameworks in place to properly protect information, educate officers on when it is not appropriate to access information, and establish effective policies and procedures to prevent it.
- Public officers who improperly access information should face disciplinary action, and in serious cases dismissal may be the appropriate sanction. Recently a number of Queensland police officers have been prosecuted for offences arising from the improper use (and sometimes disclosure) of information. Prosecution action is not reserved for police officers — any public officer should expect that, where appropriate, prosecution action will be initiated.

Sanctions for improper access

The popular image of a "computer hacker" is someone external to an agency who is attempting to gain illegal access to its computer system. But it can also apply to staff within an agency, even when they have some authorised level of access to an agency database.

Whilst often abbreviated to "computer hacking", it is important to note that, consistent with the application of the offence, its full name is "**computer hacking and misuse**".

Under legislation, public servants who access a work database for reasons not related to their official duties can be charged with computer hacking, an offence with a maximum penalty of ten years' imprisonment.

Access to a database for work reasons does not equate to unlimited access

INVESTIGATION CASE STUDY

Police officer prosecuted for computer hacking

In September 2017, Daniel Banks was found guilty of 23 charges of "computer hacking and misuse with a circumstance of aggravation". That is, he used a restricted computer without the consent of its controller, and also gained a benefit from it, namely knowledge.

Over a two-year period, Banks accessed records in relation to a number of people, including other police officers, members of his own family, the former partner of his wife and that person's associates. The records included intelligence reports, criminal and traffic histories, domestic and family violence applications and protection orders, and details of police cautions and flags. There was no evidence that the information was passed on to anyone else.

The Magistrate fined Banks $4000, noting that the police database (QPRIME) was a very powerful information tool which needed to be jealously guarded: if the system was successfully accessed for non-police purposes, the faith of the public in the integrity of police information would be eroded. Banks will now face disciplinary proceedings.

Amongst other things, the Magistrate's decision confirmed that:

- A police officer who is given access to the database does NOT have unlimited access – any access must be connected with the officer's official duties.
- In determining whether access is for official duties, conflicts of interest will be relevant, and there can be no more obvious a situation of conflict of interest than a matter involving a relation or friend.
- Mere knowledge can be a benefit under the offence provision, whether or not anything was done with the information, such as it being passed on to someone else.
- Action taken against a police officer for use contrary to Queensland Police Service protocols can be the basis for criminal proceedings, not just disciplinary proceedings.

Lessons learned

Officers employed by public agencies have access to an extraordinarily large amount of information about citizens. It will often be the case that public officers will technically be able to access all information (or all information of a particular category) on a particular database, with officers being trusted to only access information that is connected with their official duties. If an officer is determined to improperly access information, it may be very difficult to prevent it. However, if it is detected after the event, officers should expect that, at the very least, disciplinary action will follow and that in more serious cases criminal proceedings will be instituted.

It is important that agencies actively develop a culture that discourages improper access to information and does not tolerate it when it occurs. Obviously, the tone must be set at the top and be supported by education and training (upon induction to an agency and ongoing), appropriate policies and procedures (including messaging upon an officer signing into the system), and an appropriate auditing regime. Other specific measures are recommended below.

Vulnerabilities and prevention measures

The prosecution of Banks was assisted because of the framework that existed within the Queensland Police Service with respect to access to information. In addition to supporting a successful prosecution case, such measures are important in relation to preventing improper access to information and detecting non-compliances when they occur.

Potential systemic vulnerabilities	Prevention measures
Officers are unaware of the organisation's attitude to improper use of information	• Implement proper education and training (upon induction and ongoing) and keep records of training • Establish regular messaging from organisational leaders (setting the tone at the top) • Ensure that the organisation is willing to take disciplinary action and, where appropriate, refer matters to the Queensland Police Service for prosecution • Publish results of disciplinary action throughout the organisation
Officers are unclear about what constitutes improper access to information	• Implement proper education and training (upon induction and ongoing) • Establish regular messaging from organisational leaders (setting the tone at the top)
Prevention measures are not integrated into information systems	• Display warning about improper access to information and require officers to acknowledge it before signing in to systems • Require officers to enter reason for accessing information in systems • Ensure situations do not arise where officers can sign in using usernames and passwords of other officers (e.g. policies and procedures dealing with password control)
It is difficult to detect improper access to information	• Require officers to enter reason for accessing information in systems • Conduct regular audits • Encourage officers to report non-compliances • Ensure systems support proper reporting of details of access (including the information accessed)

For more information about improper access to confidential information, see: ccc.qld.gov.au/corruption-prevention/confidential-information