PREVENTION in focus

Improper access to public sector databases, no. 2

Public officers who pass information on to others lose control of the information and have no way of knowing how the information will then be used.

What you should know

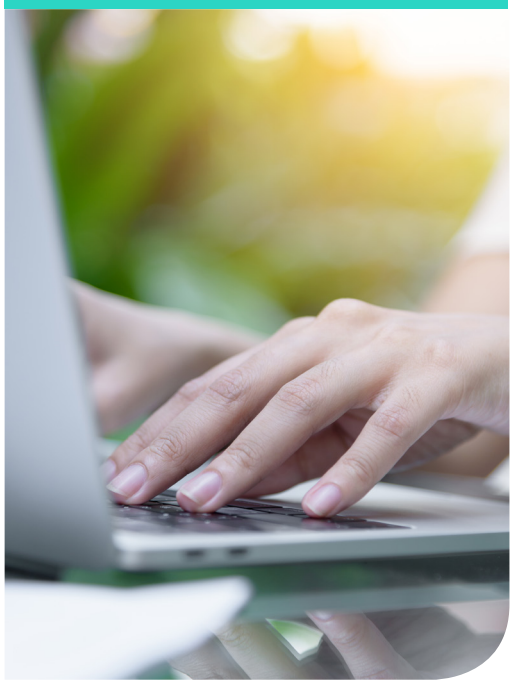
- Public officers who improperly access information should face disciplinary action and criminal prosecution and, in serious cases, dismissal may be the appropriate sanction. Whilst the media have reported a number of cases involving police officers improperly accessing information, public officers from other departments and agencies are also the subject of disciplinary and criminal action by their agencies, the CCC and the Queensland Police Service (QPS).
- A number of departments and agencies hold sensitive private information, including the QPS, Queensland Corrective Services (QCS), the Department of Transport and Main Roads, the Department of Justice and Attorney-General, Education Queensland, Queensland Health, and the Department of Child Safety, Youth and Women.
- The improper access to sensitive private information represents a serious interference with the privacy of citizens and creates reputational risks for departments and agencies. The gravity of such issues is compounded when sensitive private information is passed on to others; officers lose control of the information and its use. This was noted in a recent court decision summarised in the case study on page 2.

Misuse of confidential information is an area of focus for the CCC. In February 2018, we released our first Prevention in Focus paper on improper access to databases. This second paper on the topic, based on a recent case study, highlights that disciplinary and criminal sanctions may be imposed on public sector officers who don't follow the rules.

Crime and Corruption Commission
QUEENSLAND

May 2019

Le had displayed a cavalier attitude in thinking she had a right to access the information in the way she did.



In sentencing Le, the Magistrate noted that, once she passed the information on to her partner, she did not know what he was going to do with it and the purpose for which he would use it.

Investigation case study

Former QCS officer prosecuted for computer hacking

Lan Phuong Le commenced employment with QCS in 2009 as a senior case manager – she managed and supervised people subject to court orders. She had access to two systems – the QCS Integrated Offender Management System (IOMS) and the Queensland-Wide Interlinked Court System (QWIC). Both systems contained sensitive confidential information.

Le was in a relationship with a man for two years between 2014 and 2016. After they had separated, the man contacted the CCC and reported that Le had conducted searches of people and released the information to him.

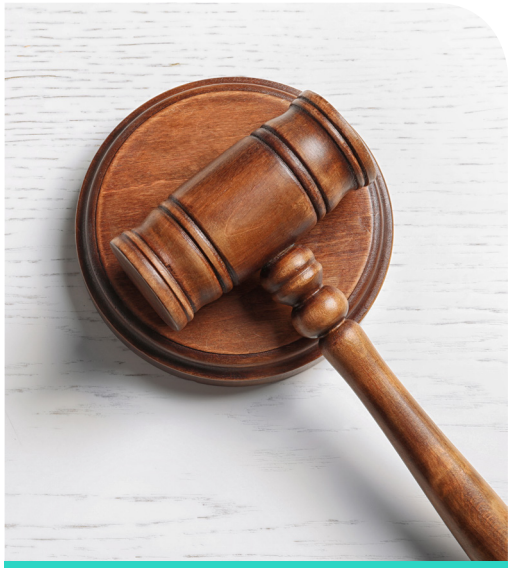
The CCC investigation revealed that over a period of around five and a half years, she searched her partner, his family members, friends and ex-partners (66 searches on 24 people in total) at the request of her partner. She also searched her old school friends (116 searches on 6 people) and other people she knew personally or through her personal life, including her brother and prospective partners. Le released various types of information to her partner about the people she searched, including their age, whether they were "in the system", details of their criminal history, whether they had been to jail, whether they had visited another person in jail and whether they had family who were in jail.

About 20 of the searches were conducted in contravention of a requirement not to conduct searches on specific people, which had been imposed after Le had made a conflict of interest declaration because she knew the people.

Le, who had no criminal history, resigned from QCS as a result of these matters.

In sentencing Le, the Magistrate noted that, once she passed the information on to her partner, she did not know what he was going to do with it and the purpose for which he would use it. The Magistrate indicated that she had thought of imposing a term of imprisonment but decided to record a conviction and impose an $8,000 fine.

The Magistrate considered it to be a serious example of the offence – Le had displayed a cavalier attitude in thinking she had a right to access the information in the way she did, it occurred over an extended period of time and not all of the offending was the result of requests from her partner. Moreover, some instances of improper access occurred after the conflict of interest process resulted in a specific restriction on her accessing information about specific people.



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.

Lessons learned

The conduct engaged in by Le in the case study would have warranted dismissal from QCS, had Le not resigned.

Public officers who 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 on the information 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 accessing confidential private information as a result of curiosity represents a serious privacy breach.

Criminal prosecution

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.

Vulnerabilities and prevention measures

In a recent survey of CCC Liaison Officers conducted by the CCC, misuse of information was a leading concern.

In February 2018's *Prevention in Focus*, potential system vulnerabilities and prevention measures were set out. Agencies should use this as a checklist. Agencies must also be aware of the potential value of the information they hold, both to their employees and to others who may seek to corrupt or exploit employees who are already inclined towards corrupt behaviour. A risk assessment should be undertaken to ensure risks are appropriately identified, analysed, evaluated and treated.

Agencies are also encouraged to consider the recent Queensland Civil and Administrative Tribunal (QCAT) decision reported as *ZIL v Queensland Police Service* [2019] QCAT 79. The QCAT Member found that, notwithstanding the measures the QPS had implemented, they were in breach of information privacy principles as all reasonable steps had not been taken to prevent unauthorised use or disclosure of personal information.

Agencies should take a risk-based approach in establishing proactive programs to audit for improper access to their databases.

The Member said, amongst other things:

> *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.* [footnotes omitted]
>
> and
>
> *They* [the QPS] *did not audit in any systemic way to supervise access even to a group of people (the victims of domestic violence) who had orders in their favour. The Service waited until there was a complaint or an incident – a time after any further potential damage to this vulnerable group. The QPS could have added to the QPrime system to allow restricted access to the information about this vulnerable group.*
>
> *They did give spasmodic web based training to staff and officers only on the responsibilities for accessing the QPrime system, but then rely on the moral fibre of an individual police officer to not access the system in circumstances (borne out by the evidence) where he knew he would not be caught – because no one looked.*

Agencies should take a risk-based approach in establishing proactive programs to audit for improper access to their databases. The availability of data analytics should be considered in this regard, especially during the development of new database systems. Such an approach will ensure agencies meet their information privacy obligations, deter would-be offenders and increase the chance of detecting offenders and, most importantly, protect the privacy of citizens.

Find out more: www.ccc.qld.gov.au/corruption-prevention/confidential-information