IPCA
Independent Police Conduct Authority
Mana Whanonga Pirihimana Motuhake

Officer's failure to recognise conflict of interest led to inappropriate use of Police database

1. On 24 July 2024 at approximately 3:00pm, Mr Z was driving on Cobham Drive in Hamilton. At a point where two lanes merge into one, Mr Z was in the outside (right) lane and Officer A (an off-duty officer) was in the inside (left) lane. Mr Z attempted to enter the merged lane but was blocked by Officer A's vehicle. Despite Officer A's vehicle being slightly ahead of Mr Z and close behind the vehicle ahead of it, Mr Z continued to move forwards into the lane ahead of Officer A's vehicle, his belief being that vehicles should always "merge like a zip" in this situation. This action forced Officer A to give way to avoid an accident. Officer A sounded his horn, gave Mr Z 'the finger', and tailgated Mr Z for some time until they were separated by traffic. Officer A took note of Mr Z's vehicle registration.

2. The following day while on duty, Officer A sought advice from a more senior officer about what he should do in relation to Mr Z's manner of driving. The senior officer advised him to look up the vehicle registration on the Police database and give Mr Z an 'educational call'. Following this advice, Officer A accessed the Police database and, using Mr Z's vehicle registration, obtained Mr Z's contact information. He then used that information to telephone Mr Z to discuss the incident and his driving. The call became heated, and Mr Z says that Officer A threatened him with legal action for driving dangerously.

3. Mr Z complained to Police about Officer A's actions. Police completed an employment investigation, which the Authority oversaw.

4. We also undertook an independent investigation into the matter, examining whether Officer A correctly managed his conflict of interest and whether his use of the Police database was authorised.

5. Our investigator considered the law in relation to accessing a computer system for a dishonest purpose; reviewed Police values and policies; and interviewed Mr Z, Officer A, and three other Police staff.

Did Officer A access a computer system for a dishonest purpose?

6. To meet the requirements of section 249 of the Crimes Act 1961, a person must access a computer system dishonestly and must obtain a benefit. Case law is clear that a benefit includes the acquiring of knowledge or information to which one was not otherwise entitled.[1]

7. The definition of "dishonestly" is also addressed in the cases. One definition is that: *"'Dishonestly' requires an absence of belief that there was consent or authority to (in this case) download the data. It is not necessary to prove that the belief was reasonable."* [2]

8. Here, Officer A did obtain a benefit from accessing the Police computer in that he obtained Mr Z's contact information that he would not otherwise have known. However, Officer A sought advice from a senior officer and, it appears, genuinely believed from that conversation that he was authorised to download the information. We accept that he did not act dishonestly when accessing the information and therefore his actions are not a breach of section 249.

Did Officer A breach any relevant Police policies?

9. We also assessed Officer A's behaviour against two Police policies: the Managing Conflicts of Interest policy and the Information Security policy regarding acceptable use of information and ICT.

10. The public expects Police to carry out its work impartially at all times. Officer A was personally involved in the traffic incident. As such, he had a conflict of interest in the Police handling of this matter because his personal interests could - or could be seen to - interfere with his ability to be impartial, objective, and independent.

11. Officer A showed a distinct lack of understanding of actual and perceived conflicts of interest and did not recognise the conflict of interest in this incident. Although it is apparently common practice for Police to contact people and speak to them about their driving, it was inappropriate in the circumstances for Officer A to be the officer contacting Mr Z.

12. The Information Security policy states that officers must not collect, access, use or attempt to use any information held by Police unless it is for a lawful policing purpose or duty. Officer A's lack of understanding around conflicts of interest led him to the mistaken view that he was using the Police database for legitimate work purposes.

13. Police policy states that any conflict of interest must be raised with a supervisor. Although Officer A was not conscious of his conflict of interest, he did explain the situation to a more senior officer and seek his advice. Officer A also obtained authorisation from that senior officer to access Mr Z's contact details. That authorisation was not soundly based. However, because Officer A did raise the issue with a senior officer and did obtain authority to access the information, our assessment is that he did not breach Police policy.

---

[1] Police v Le Roy (HC, 2006).
[2] Watchorn v R (CA, 2014).

14. The fact that the senior officer also failed to appreciate the obvious conflict of interest, and failed to advise Officer A to hand the matter over to someone else to deal with, he too demonstrated poor judgement and decision making.

15. At interview, Officer A ultimately accepted the incident involved a conflict of interest and that he could have handled the matter differently. We suggest Officer A and the senior officer involved in this matter seek further training in relation to Police's Managing Conflicts of Interest policy to avoid similar situations in the future.

Judge Kenneth Johnston KC

Chair
Independent Police Conduct Authority

20 November 2025

IPCA: 24-23692