CORRUPTION PREVENTION CONCEPTS: UNAUTHORISED DISCLOSURE OF INFORMATION

Australian Government
Australian Commission for Law Enforcement Integrity

To perform their duties, law enforcement officers are afforded privileged access to sensitive information. This includes operational information and criminal intelligence, in addition to knowledge of investigative methodologies and technical capabilities.

ACLEI investigations have identified the unauthorised disclosure of information – to criminal entities, the media, family and friends, and other parties – as a key corruption risk for law enforcement agencies. Serious and organised criminal entities place a high value on law enforcement information and actively seek to corrupt officers – through bribery, extortion and other means – for access.

Unauthorised disclosure of information

An unauthorised disclosure occurs when a Commonwealth officer, whether deliberately or inadvertently, makes information (including documents and other things) available or accessible to others without having the authority to do so. Unauthorised disclosure may sometimes be referred to as 'a leak' and may constitute corrupt conduct.

In a law enforcement environment, unauthorised disclosures commonly relate to the dissemination of information pertaining to individuals or groups; law enforcement operations, capability and methodology; and systemic vulnerabilities in law enforcement capability and capacity[1].

It is an offence for a Commonwealth officer (or persons performing services for or on behalf of the Commonwealth) to communicate any information or publish any document which comes into their knowledge or possession (except when authorised to do so)[2].

> ACLEI investigations have uncovered allegations of law enforcement officers leaking operational information to criminal entities to assist their associates evade detection, or for a monetary benefit.

Information obtained by Commonwealth officers in the course of their duties may be extremely valuable to criminal entities and other external parties, such as business entities seeking to obtain a commercial advantage over their competitors[3].

An officer may knowingly disclose information to criminal entities or external parties for personal benefit (monetary or otherwise)[4]. Alternatively, unauthorised disclosures may be for a 'noble cause' or politically motivated[5].

Unauthorised disclosures may have significant and long-lasting effects on agencies, their employees, governments at all levels, and the wider Australian community. This may include substantial reputational damage for the agency in question and, in extreme circumstances, compromise of Australia's national security interests.

---

[1] ACLEI 2019 - https://www.aclei.gov.au/corruption-prevention/key-concepts/glossary
[2] Section 122.4, Unauthorised disclosure of information by current and former Commonwealth officers etc. https://www.legislation.gov.au
[3] ACLEI 2019 - https://www.aclei.gov.au/corruption-prevention/key-concepts/nature-corruption
[4] ACLEI 2019 - https://www.aclei.gov.au/corruption-prevention/key-concepts/understanding-risk
[5] Porter & Warrender 2009 *A multivariate model of police deviance: examining the nature of corruption, crime and misconduct* Policing and Society, Griffith Research Online - https://doi.org/10.1080/10439460802457719

What you need to know:

High risk area — criminal targeting

Law enforcement officers have access to sensitive and operational information which is valuable to criminal entities. These entities use sophisticated methods to target and corrupt law enforcement officers, including **grooming**, to exploit the privileged access and information they hold[6].

Information misuse is a key enabler of organised crime groups[7]. Criminal entities may seek access to law enforcement information that enables them to evade detection or exploit specific law enforcement vulnerabilities.

Grooming is the deliberate targeting of law enforcement officers by outside parties seeking access to law enforcement through intimate relationships, family connections, or cultural and social links. Organised crime entities may attempt to compromise officer loyalty to their employer by exploiting their relationship, usually over an extended period of time.

High risk area – law enforcement subcultures

The nature of law enforcement work can create an intense group loyalty, which can be maintained in the face of corruption by colleagues and at the expense of the expectations of the agency. This loyalty can endure after officers leave law enforcement employment, allowing them inappropriate access to information or law enforcement decision-making.

An ACLEI investigation showed that a former law enforcement officer had used their relationships with current serving officers to gain access to sensitive information – in some cases for the use of serious and organised criminal entities.

Reach-back occurs when former law enforcement employees seek out currently-serving employees to provide favours, access, or information[8].

The movement of officers between law enforcement agencies can also compound the risks of unauthorised disclosure.

Officers may believe they are adding value or contributing to the new employer's knowledge base by seeking or sharing information with former colleagues, when in fact they may be breaching operational security and placing operations or people at risk.

High risk area — inadvertent disclosures

Officers may inadvertently disclose sensitive information when discussing their work and duties in an unsecured environment, for example with family and friends and online via social media.

Inadvertent disclosures to family, friends and associates may pose a significant risk where information is subsequently on-disclosed to others[9], particularly where the scope of the disclosure is unknown.

Officers at all levels may use social media or networking sites to discuss work activities or maintain contact with colleagues outside of work hours. Maintaining custody of information that is uploaded to social media platforms may be extremely difficult as data may be stored internationally and accessed by third parties without the knowledge of or consent of the officer[10].

An officer may also inadvertently leak information on social media if they are voicing negative opinions about their agency, including agency processes or policies. Certain privacy restrictions on social media sites

ACLEI have identified instances where law enforcement officers have shared sensitive information on social media or other information sharing platforms.

[6] ACLEI 2019 - https://www.aclei.gov.au/corruption-prevention/key-concepts/grooming
[7] ibid
[8] ACLEI 2018 - https://aclei.govcms.gov.au/sites/default/files/18362_-_aclei_-_corruption_prevention_final.pdf?acsf_files_redirect
[9] Goldsmith 2013 *Disgracebook policing: social media and the rise of police indiscretion* Policing and Society. Taylor and Francis Online - https://doi.org/10.1080/10439463.2013.864653
[10] Rose 2011 *The Security Implications of Ubiquitous Social Media* International Journal of Management & Information Systems https://pdfs.semanticscholar.org/a96f/dd049e21696814389ea306b7bb9dffa52e74.pdf

may make it difficult for an agency to detect information leaks or inappropriate information disclosures[11].

Law enforcement officers who upload detailed personal information to their social media accounts and networking sites, such as LinkedIn, may become potential targets for coercion by criminal entities[13].

ACLEI Case Study Example

During an ACLEI investigation into the disclosure of classified information to associates of an outlaw motorcycle gang (OMCG) it was found that the daughter of a law enforcement officer may have inadvertently disclosed information within a group of OMCG-associated members[12]. Information shared in the group sparked rumours that law enforcement was targeting specific OMCG members and their associates as they travelled in and out of Australia.

The officer participated in a record of interview, under criminal caution, with ACLEI investigators. The officer acknowledged that their daughter was aware of their employment and would have gained a general understanding of their day-to-day functions and duties.

Of concern to ACLEI investigators was the genuine risk of compromise to the officers' daughter arising from peer group, social, and other pressures. There was also a risk that the daughter's associations could lead to OMCG members coercing the law enforcement officer into corrupt conduct through direct or implied threats of harm to the officer's daughter.

High risk area – 'noble cause' disclosures

The risks of unauthorised disclosure may increase in circumstances where an officer feels that a social, moral or ethical issue exists which can be addressed by leaking information[14].

Similarly, officers with strong individual values and beliefs which run counter to certain agency decisions may disclose confidential information to generate public scrutiny or potentially sabotage the decision in question[15].

The officer may justify their conduct to act unlawfully because they believe it is for the 'right reasons' or the 'greater good'[16].

Officers may also be more likely to leak information if they believe established reporting mechanisms are inadequate to manage or investigate their concerns.

ACLEI investigations have uncovered instances of law enforcement officers sending classified departmental information to other external agencies with the intent of bringing internal departmental matters to the attention of the media and the public.

High risk area — technology in the workplace

ACLEI investigations have identified instances where law enforcement officers have shared operational information and documents via text messages and social media.

The increased use of personal electronic devices in the workplace may increase the risk of unauthorised disclosure, given the ease and speed by which large quantities of information can be disseminated[17].

Smart phones equipped with cameras may also make it easier for officers to capture sensitive or operational information, while encrypted communications technology may limit the ability of

[11] Molok, Chang & Ahmad 2010 *Information leakage through Online Social Networking: Opening the Doorway for Advanced Persistence Threats* Edith Cowan University https://doi.org/10.4225/75/57b673cf34781
[12] ACLEI 2017 - https://www.aclei.gov.au/Corruption-prevention/case-studies/case-study-4-integrity-risk
[13] Smith, Oberman, Fuller & Sergi 2018 *Understanding and responding to serious and organised crime involvement in public sector corruption* Trends & Issues in Crime & Criminal Justice http://eds.a.ebscohost.com/eds/pdfviewer/pdfviewer?vid=2&sid=619201d0-87e7-45ff-ac29-e8cd35291f91%40sessionmgr4007
[14] Goldsmith 2013 *Disgracebook policing: social media and the rise of police indiscretion* Policing and Society. Taylor and Francis Online - https://doi.org/10.1080/10439463.2013.864653
[15] Gelber 2019 *The precarious protection of free speech in Australia: the Banjeri case* Australian Journal of Human Rights https://doi.org/10.1080/1323238X.2019.1690833
[16] Gottschalk 2008 *Policing police crime: the case of criminals in the Norwegian police* International Journal of Police Science & Management https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/injposcim11&section=46
[17] IBAC 2019 - Unauthorised access and disclosure of information held by Victoria Police - https://www.ibac.vic.gov.au/docs/default-source/research-documents/unauthorised-access-and-disclosure-of-information-held-by-victoria-police.pdf?sfvrsn=1283ccb8_4

agencies to identify and substantiate the source of information disclosures.

What should you do?

For agencies:

- Consider the information you hold and regularly review information security controls to ensure they remain fit for purpose – identify and protect your information 'crown jewels'.
- Maintain appropriate oversight and audit controls over information and communications systems.
- Ensure officer training and awareness programs remain contemporary and align with agency expectations regarding information management obligations and responsibilities.
- Encourage staff to report integrity matters, including real or perceived information disclosures.
- Consider the appropriateness of employees utilising personal electronic devices in the workplace, particularly where employees regularly access sensitive information as part of their duties.

For managers:

- Reinforce agency expectations regarding the appropriate management, access and use of sensitive and operational information.
- Consider what information employees in your work area have access to and identify whether additional information security control measures may be required.
- Encourage employees to refresh their knowledge on information management and classified document handling procedures.
- Foster an environment where your employees are empowered to ask questions, seek advice, and raise concerns.

For employees:

- Understand the value of the information held by your agency and who may seek to exploit this information.
- Report all actual or suspected information leaks to your agency as soon as possible.
- Maintain a level of security awareness even when in the company of family and close friends—who else might they be talking to? Do they have a need to know?
- Trust established reporting mechanisms in your agency – these mechanisms exist to mitigate the risk to yourself and your agency.
- Know where to go for help and advice within your agency – your integrity and professional standards area or your manager are good places to start.

Further information and resources:

- Watch the ACLEI Corruption Prevention Concepts Video: Unauthorised Disclosure
- ACLEI Corruption Prevention Posters: available for download from the ACLEI website
- Investigation Summary Report - Operation Hadron
- Investigation Report - Operation Marlowe
- ACLEI Case Study 4 - Allegation a law enforcement officer released classified information
- ACLEI website – developing risk control plans

Australian Government

Australian Commission for
Law Enforcement Integrity

Report corruption at:

aclei.gov.au