Australian Capital Territory

Workplace Privacy Act 2011

A2011-4

Republication No 4

Effective: 14 October 2016

Republication date: 14 October 2016

Last amendment made by A2016-37
(republication for amendments by A2016-22
as amended by A2016-37)

Authorised by the ACT Parliamentary Counsel

About this republication

The republished law

This is a republication of the *Workplace Privacy Act 2011* (including any amendment made under the *Legislation Act 2001*, part 11.3 (Editorial changes)) as in force on 14 October 2016. It also includes any commencement, amendment, repeal or expiry affecting this republished law to 14 October 2016.

The legislation history and amendment history of the republished law are set out in endnotes 3 and 4.

Kinds of republications

The Parliamentary Counsel's Office prepares 2 kinds of republications of ACT laws (see the ACT legislation register at www.legislation.act.gov.au):

- authorised republications to which the *Legislation Act 2001* applies
- unauthorised republications.

The status of this republication appears on the bottom of each page.

Editorial changes

The *Legislation Act 2001*, part 11.3 authorises the Parliamentary Counsel to make editorial amendments and other changes of a formal nature when preparing a law for republication. Editorial changes do not change the effect of the law, but have effect as if they had been made by an Act commencing on the republication date (see *Legislation Act 2001*, s 115 and s 117). The changes are made if the Parliamentary Counsel considers they are desirable to bring the law into line, or more closely into line, with current legislative drafting practice.

This republication includes amendments made under part 11.3 (see endnote 1).

Uncommenced provisions and amendments

If a provision of the republished law has not commenced, the symbol **U** appears immediately before the provision heading. Any uncommenced amendments that affect this republished law are accessible on the ACT legislation register (www.legislation.act.gov.au). For more information, see the home page for this law on the register.

Modifications

If a provision of the republished law is affected by a current modification, the symbol **M** appears immediately before the provision heading. The text of the modifying provision appears in the endnotes. For the legal status of modifications, see the *Legislation Act 2001*, section 95.

Penalties

At the republication date, the value of a penalty unit for an offence against this law is $150 for an individual and $750 for a corporation (see *Legislation Act 2001*, s 133).

Australian Capital Territory

Workplace Privacy Act 2011

Contents

Australian Capital Territory

Workplace Privacy Act 2011

An Act to regulate surveillance of workers in workplaces, and for other purposes

Part 1 Preliminary

1 Name of Act

This Act is the *Workplace Privacy Act 2011*.

3 Dictionary

The dictionary at the end of this Act is part of this Act.

Note 1 The dictionary at the end of this Act defines certain terms used in this Act, and includes references (***signpost definitions***) to other terms defined elsewhere.

For example, the signpost definition '***adverse action***—see the *Fair Work Act 2009* (Cwlth), section 342.' means that the term 'adverse action' is defined in that section and the definition applies to this Act.

Note 2 A definition in the dictionary (including a signpost definition) applies to the entire Act unless the definition, or another provision of the Act, provides otherwise or the contrary intention otherwise appears (see Legislation Act, s 155 and s 156 (1)).

4 Notes

A note included in this Act is explanatory and is not part of this Act.

Note See the Legislation Act, s 127 (1), (4) and (5) for the legal status of notes.

5 Offences against Act—application of Criminal Code etc

Other legislation applies in relation to offences against this Act.

Note 1 *Criminal Code*

The Criminal Code, ch 2 applies to all offences against this Act (see Code, pt 2.1).

The chapter sets out the general principles of criminal responsibility (including burdens of proof and general defences), and defines terms used for offences to which the Code applies (eg ***conduct***, ***intention***, ***recklessness*** and ***strict liability***).

Note 2 *Penalty units*

The Legislation Act, s 133 deals with the meaning of offence penalties that are expressed in penalty units.

Part 2 Object and important concepts

6 Object of Act

The main object of this Act is to regulate the collection and use of workplace surveillance information.

7 Meaning of *worker*

In this Act:

worker means an individual who carries out work in relation to a business or undertaking, whether for reward or otherwise, under an arrangement with the person conducting the business or undertaking.

Examples—worker

1 employee

2 independent contractor

3 outworker

4 person doing a work experience placement

5 volunteer

Note An example is part of the Act, is not exhaustive and may extend, but does not limit, the meaning of the provision in which it appears (see Legislation Act, s 126 and s 132).

8 Meaning of *employer*

(1) In this Act:

employer, of a worker—

(a) includes—

(i) a person who engages the worker to carry out work in the person's business or undertaking; and

(ii) if the person who engages the worker is a corporation—a related body corporate of the corporation; but

(b) does not include a person (the ***householder***) who engages someone else to perform domestic duties at the premises where the householder lives.

Examples—employer

1 principal contractor is an employer of a subcontractor

2 host organisation is an employer of a labour hire worker

Note An example is part of the Act, is not exhaustive and may extend, but does not limit, the meaning of the provision in which it appears (see Legislation Act, s 126 and s 132).

(2) In this section:

related body corporate—see the Corporations Act, section 9.

9 Meaning of business or undertaking

In this Act:

business or undertaking includes—

(a) a not-for-profit business; and

(b) an activity conducted by a local, state or territory government.

10 Meaning of *workplace*

In this Act:

workplace means a place where work is, has been, or is to be, carried out by or for someone conducting a business or undertaking.

11 Meaning of *surveillance* etc

(1) In this Act:

conduct surveillance—a person ***conducts*** surveillance if the person—

(a) conducts the surveillance personally; or

(b) causes someone else to conduct the surveillance.

data surveillance device—

(a) means a device or program capable of being used to record or monitor the input of information into or the output of information from a computer; but

(b) does not include an optical surveillance device.

optical surveillance device—

(a) means a device capable of being used to record visually or observe an activity; but

(b) does not include spectacles, contact lenses or a similar device used by a person with impaired sight to overcome that impairment.

surveillance means surveillance using a surveillance device.

surveillance device means—

(a) a data surveillance device, an optical surveillance device or a tracking device; or

(b) a device that is a combination of any 2 or more of the devices mentioned in paragraph (a); or

(c) a device of a kind prescribed by regulation.

tracking device means an electronic device capable of being used to work out or monitor the location of a person or an object or the status of an object.

Examples—tracking device

GPS, biometrics, radio frequency identification

Note An example is part of the Act, is not exhaustive and may extend, but does not limit, the meaning of the provision in which it appears (see Legislation Act, s 126 and s 132).

(2) In this section:

device includes an instrument, apparatus or equipment.

Part 3 Notified surveillance

Division 3.1 General

12 Meaning of *surveillance*—pt 3

In this part:

surveillance does not include—

(a) covert surveillance; or

(b) prohibited surveillance.

Note ***Covert surveillance***—see s 24.
Prohibited surveillance—see the dictionary.

Division 3.2 Notifying workplace surveillance

13 Notice of surveillance required

(1) An employer may only conduct surveillance of a worker in a workplace if—

(a) the employer gives written notice to the worker under this section; and

Note For how documents may be given, see the Legislation Act, pt 19.5.

(b) the surveillance is conducted in accordance with the notice.

(2) However, an employer need not give written notice to a worker for surveillance using an optical surveillance device in a workplace if the workplace is not a usual workplace of the worker.

(3) The notice must be given—

(a) at least 14 days before the surveillance starts; or

(b) if the worker agrees to a period of less than 14 days for giving the notice—within the agreed lesser period; or

(c) if a new worker starts work with an employer that already conducts surveillance or will start conducting surveillance in less than 14 days after the new worker starts work—before the new worker starts work.

(4) The notice must state—

(a) the kind of surveillance device to be used for the surveillance; and

(b) how the surveillance will be conducted; and

(c) who will regularly or ordinarily be the subject of the surveillance; and

(d) when the surveillance will start; and

(e) whether the surveillance will be continuous or intermittent; and

(f) whether the surveillance will be for a stated period or ongoing; and

(g) the purpose for which the employer may use and disclose surveillance records of the surveillance; and

(h) that the worker may consult with the employer about the conduct of the surveillance under section 14.

(5) A notice may be in the form of a policy of the employer or otherwise.

14 Requirement for consultation on proposed surveillance

(1) This section applies if an employer must give a worker notice under section 13.

(2) The employer must consult with the worker in good faith about the conduct of the surveillance for not less than the notice period mentioned in section 13 (3).

(3) For this section, an employer consults with the worker ***in good faith*** if the employer gives the worker a genuine opportunity to influence the conduct of the surveillance.

15 Additional requirements for optical surveillance devices

(1) An employer may only conduct surveillance of a worker using an optical surveillance device if—

(a) the optical surveillance device used for the surveillance is clearly visible in the workplace where the surveillance is conducted; and

(b) a sign is clearly visible at each entrance to the workplace, telling people that they may be under surveillance in the workplace.

(2) In this section:

optical surveillance device includes a camera casing or other equipment that generally indicates the presence of an optical surveillance device.

16 Additional requirements for data surveillance devices

(1) An employer may only conduct surveillance of a worker using a data surveillance device if—

(a) the surveillance is conducted in accordance with a policy of the employer on surveillance of workers in the workplace using data surveillance devices; and

(b) the employer has notified the worker, before conducting the surveillance, of the policy in a way that it is reasonable to assume that the worker is aware of and understands the policy.

(2) For subsection (1) (a), the policy must state—

(a) how the employer's computer resources may, and must not, be used; and

(b) what information about the use of the employer's computer resources is logged and who may access the logged information; and

(c) how the employer may monitor and audit a worker's compliance with the policy.

(3) In this section:

computer resources includes internet access and electronic communication applications.

17 Additional requirements for tracking devices

(1) An employer may only conduct surveillance of a worker that involves the tracking of a vehicle or other thing using a tracking device if there is a notice clearly visible on the vehicle or other thing stating that the vehicle or thing is being tracked.

(2) However, subsection (1) does not apply if—

(a) it is not reasonably practicable to have a notice on the vehicle or other thing; and

(b) the employer has taken reasonable steps to notify workers that the vehicle or other thing is being tracked.

18 Offences—failure to comply with notified surveillance requirements

(1) An employer commits an offence if the employer—

(a) is required to notify a worker of surveillance under section 13; and

(b) the employer fails to comply with a requirement under section 13 in relation to the surveillance.

Maximum penalty: 20 penalty units.

(2) An employer commits an offence if the employer—

(a) conducts surveillance of a worker using an optical surveillance device; and

(b) fails to comply with a requirement under section 15 in relation to the surveillance.

Maximum penalty: 20 penalty units.

(3) An employer commits an offence if the employer—

(a) conducts surveillance of a worker using a data surveillance device; and

(b) fails to comply with a requirement under section 16 in relation to the surveillance.

Maximum penalty: 20 penalty units.

(4) An employer commits an offence if the employer—

(a) conducts surveillance of a worker using a tracking device; and

(b) fails to comply with a requirement under section 17 in relation to the surveillance.

Maximum penalty: 20 penalty units.

Division 3.3 Other matters

19 Surveillance by agreement

(1) Surveillance of a worker is taken to comply with the requirements of this part if—

(a) the worker agrees to the conduct of the surveillance for a purpose other than surveillance of the worker; and

(b) the surveillance is conducted in accordance with the agreement.

(2) For this section, a worker is taken to agree to the conduct of surveillance if a body representing a substantial number of workers in the workplace agrees to the conduct of the surveillance.

20 Offence—restrictions on blocking electronic communication and internet access

(1) An employer commits an offence if the employer stops the delivery of an electronic communication sent to or by a worker, or stops a worker's access to a website.

Maximum penalty: 5 penalty units.

Note ***Electronic communication***—see the dictionary.

(2) Subsection (1) does not apply if—

(a) the employer is acting in accordance with a policy of the employer on electronic communication and internet access; and

(b) the employer—

(i) notified the worker, before stopping delivery of the electronic communication or access to the website, of the policy in a way that it is reasonable to assume that the worker is aware of and understands the policy; or

(ii) was not required to notify the worker under section 21 (2) or (3).

Note The employer has an evidential burden in relation to the matters mentioned in s (2) (see Criminal Code, s 58).

21 Notice of blocking electronic communication and internet access

(1) If an employer stops delivery of an electronic communication under section 20 (2), the employer must give the worker a notice (a ***stopped delivery notice***) that delivery of the electronic communication has been stopped as soon as practicable after it is stopped.

Note ***Electronic communication***—see the dictionary.

(2) However, an employer is not required to give a worker a stopped delivery notice if delivery of the electronic communication is stopped—

(a) because the employer believes the electronic communication is—

(i) a communication that is a commercial electronic message within the meaning of the *Spam Act 2003* (Cwlth); or

(ii) a communication or attachment that might result in an unauthorised interference with, or damage to, the operation of—

(A) a computer or computer network operated by the employer; or

(B) a program run by a computer or computer network of the employer; or

(C) data stored on a computer or computer network of the employer; or

(iii) a communication or attachment that might reasonably be considered to be threatening, harassing or offensive; or

(b) by the operation of a software program designed to stop a communication of a type mentioned in paragraph (a).

(3) Also, an employer is not required to give a worker a stopped delivery notice for an electronic communication sent by the worker if the employer was not, and could not reasonably be expected to be, aware—

(a) of the identity of the worker who sent the communication; or

(b) that the communication was sent by a worker.

(4) An employer's policy on electronic communication and internet access must not provide for delivery of an electronic communication or access to a website to be stopped only because—

(a) the communication was sent by or on behalf of an industrial association of a worker or an officer of an industrial association; or

(b) the communication or a website contains information relating to industrial matters.

(5) In this section:

industrial association—see the *Fair Work Act 2009* (Cwlth), section 12.

industrial matters means matters or things affecting or relating to work done or to be done in an industry, or the rights or obligations of employers or workers in an industry.

22 Offences—use and disclosure of surveillance records

(1) An employer commits an offence if the employer—

(a) conducts surveillance of a worker; and

(b) uses a surveillance record in relation to the surveillance to take adverse action against the worker.

Maximum penalty: 50 penalty units.

Note ***Adverse action***—see the *Fair Work Act 2009* (Cwlth), s 342.

(2) Subsection (1) does not apply if the notice given to the worker under section 13 stated that the employer may use the surveillance to take adverse action against the worker.

(3) An employer who conducts surveillance of a worker in a workplace must ensure that a surveillance record in relation to the surveillance is otherwise only used or disclosed if—

(a) the record is used or disclosed for a legitimate purpose in relation to the employment of a worker or the legitimate business activities or functions of the employer; or

(b) the record is disclosed to a member of a law enforcement agency for use in connection with the detection, investigation or prosecution of an offence; or

(c) the record is used or disclosed for a purpose directly or indirectly related to a civil or criminal proceeding; or

(d) the employer reasonably believes that the use or disclosure of the record is necessary to avoid an imminent risk of death of, or serious injury to, someone or substantial damage to property; or

(e) the record is disclosed under section 23.

Maximum penalty: 50 penalty units.

23 Access to surveillance records of notified surveillance

(1) An employer must, on the written request of a worker, allow the worker to have access to surveillance records in relation to the worker.

(2) If an employer fails to allow the worker to have access to surveillance records under subsection (1), the records must not be used by the employer—

(a) in a legal proceeding between the employer and the worker; or

(b) to take adverse action against the worker.

Note ***Adverse action***—see the *Fair Work Act 2009* (Cwlth), s 342.

(3) Subsections (1) and (2) do not apply if—

(a) disclosing the surveillance records would be an offence under section 22 or otherwise unlawful; or

(b) the employer is satisfied on reasonable grounds that—

(i) allowing access would have an unreasonable impact on the privacy of other individuals; or

(ii) the request for access is frivolous or vexatious; or

(iii) the information relates to existing or anticipated legal proceedings between the employer and the worker and the information would be accessible by the process of discovery in those proceedings; or

(iv) allowing access would reveal the intentions of the employer in relation to negotiations with the individual in a way that would be likely to prejudice the negotiations; or

(v) not allowing access is required or authorised under a territory law or the law of another jurisdiction; or

(vi) allowing access would be likely to prejudice an investigation of possible unlawful activity; or

(vii) allowing access would be likely to prejudice—

(A) the prevention, detection, investigation, prosecution or punishment of a criminal offence or breach of a law imposing a penalty or sanction; or

(B) the enforcement of a law relating to the confiscation of the proceeds of crime; or

(C) the prevention, detection, investigation or remedying of serious improper conduct; or

(D) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders, by or on behalf of a law enforcement agency; or

(c) a law enforcement body performing a lawful security function asks the employer not to allow access to the information on the basis that allowing access would be likely to cause damage to the security of Australia.

Part 4 Covert surveillance

Division 4.1 General

24 Meaning of covert surveillance—Act

In this Act:

covert surveillance—

(a) means surveillance of a worker in a workplace conducted by an employer without notifying the worker under part 3 (Notified surveillance); but

(b) does not include prohibited surveillance.

25 Definitions—pt 4

In this part:

covert surveillance authority—see section 26.

covert surveillance record means a surveillance record in relation to covert surveillance.

surveillance supervisor, for a covert surveillance authority, means a person named in a covert surveillance authority as responsible for overseeing the conduct of the authorised covert surveillance.

unlawful activity means an act or omission that is an offence against a law in force in the Territory.

Division 4.2 Covert surveillance authorities

26 Application for covert surveillance authority

(1) An employer may apply to the Magistrates Court for authority (a ***covert surveillance authority***) to conduct covert surveillance of a worker in a workplace only for the purpose of finding out if the worker is engaged in an unlawful activity in the workplace.

Note 1 If a form is approved under the *Court Procedures Act 2004*, s 8 for the application, the form must be used.

Note 2 A fee may be determined under the *Court Procedures Act 2004*, s 13 for this provision.

(2) The application must be in writing and be accompanied by particulars of—

(a) the grounds that the employer has for suspecting a worker is involved in an unlawful activity and the name of the worker (if practicable); and

(b) the actions (if any) the employer has taken to detect the unlawful activity and the result of the actions; and

(c) the name of any worker (if practicable) or a description of the group or class of workers, who will regularly or ordinarily be the subject of the covert surveillance; and

(d) a description of the premises, place, computer, vehicle or other thing that will regularly or ordinarily be the subject of the covert surveillance; and

(e) the kind of surveillance device that is proposed to be used for the covert surveillance; and

(f) the period during which the covert surveillance is proposed to be conducted; and

(g) if an application for a covert surveillance authority for the proposed surveillance has previously been made—the result of the application and, if the authority was issued, any covert surveillance conducted under the authority; and

(h) anything else prescribed by regulation.

(3) An application must also nominate at least 1 person to be a surveillance supervisor for the covert surveillance authority.

(4) If an application for a covert surveillance authority is refused by the Magistrates Court, a further application in relation to the same surveillance may only be made if the further application provides additional relevant information.

27 Hearing in private

A hearing of an application for a covert surveillance authority must be held in private.

28 Issuing covert surveillance authority

(1) The Magistrates Court may, on application, issue a covert surveillance authority if satisfied that there are reasonable grounds to issue the authority.

Note If a form is approved under the *Court Procedures Act 2004*, s 8 for the order, the form must be used.

(2) In considering whether there are reasonable grounds to issue the covert surveillance authority, the Magistrates Court must consider—

(a) the seriousness of the suspected unlawful activity; and

(b) whether and the extent to which the proposed surveillance might intrude on the worker's or someone else's privacy; and

(c) if the proposed surveillance may be conducted in a non-work area—a worker's heightened expectation of privacy in the area; and

Note 1 Surveillance is prohibited in some non-work areas (see s 41).

Note 2 ***Non-work area***—see the dictionary.

(d) whether there are other appropriate ways to find out if the worker is engaged in an unlawful activity in the workplace; and

(e) whether it is more appropriate for the suspected unlawful activity to be investigated by a law enforcement agency; and

(f) whether the person nominated to be the surveillance supervisor in the application is suitable.

Note Section 29 deals with appointing a surveillance supervisor.

(3) The Magistrates Court may consider any other relevant matter.

(4) The covert surveillance authority must state—

(a) the nature of the suspected unlawful activity and the name of the worker (if practicable) in relation to which the authority is issued; and

(b) the name of any worker (if practicable) or a description of the group or class of workers who may be the subject of the covert surveillance; and

(c) the premises, place, computer, vehicle or other thing that may be the subject of the covert surveillance; and

(d) the kind of surveillance device that may be used for the covert surveillance and where the device may be used or installed; and

(e) when the covert surveillance may be conducted; and

(f) the name of each person designated as a surveillance supervisor; and

(g) the period that the authority remains in force; and

(h) the conditions on the covert surveillance authority; and

Note For the conditions on a covert surveillance authority, see s 31.

(i) the requirements for—

(i) reporting on the use of the covert surveillance authority under section 37; and

(ii) use and disclosure of covert surveillance records under section 39.

29 Appointing surveillance supervisor

(1) The Magistrates Court must appoint at least 1 person to be the surveillance supervisor in relation to a covert surveillance authority.

(2) The Magistrates Court may appoint a person to be the surveillance supervisor only if satisfied that the person—

(a) has the experience or expertise to qualify the person to be a surveillance supervisor; and

(b) is independent of the employer; and

Example

the person is not an employee of the employer

Note An example is part of the Act, is not exhaustive and may extend, but does not limit, the meaning of the provision in which it appears (see Legislation Act, s 126 and s 132).

(c) if the covert surveillance authority allows surveillance to be conducted in a non-work area—is able to adequately accommodate a worker's heightened expectation of privacy in the area.

Note 1 Surveillance is prohibited in some non-work areas (see s 41).

Note 2 ***Non-work area***—see the dictionary.

30 Duration of covert surveillance authority

A covert surveillance authority may be issued for not longer than 30 days or another period prescribed by regulation.

31 Conditions on covert surveillance authority

(1) A covert surveillance authority is subject to the conditions mentioned in this section.

(2) A surveillance supervisor must not give another person access to a covert surveillance record.

(3) However, a surveillance supervisor may give an employer a part of a covert surveillance record—

(a) for a purpose for which the covert surveillance authority was issued; or

(b) to identify or detect any other unlawful activity in a workplace.

(4) A surveillance supervisor must, within 3 months after the expiry of a covert surveillance authority, erase or destroy all covert surveillance records in relation to the authority, other than records required for investigative or evidentiary purposes.

(5) An employer must, on the written request of a worker, give the worker access to any part of a covert surveillance record that an employer seeks to rely on to take adverse action in relation to the worker.

Note ***Adverse action***—see the *Fair Work Act 2009* (Cwlth), s 342.

32 Defects in covert surveillance authority

A defect in a covert surveillance authority does not invalidate the authority unless the defect affects the substance of the authority in a material particular.

33 Varying or cancelling covert surveillance authority

(1) The Magistrates Court may, at any time, vary or cancel a covert surveillance authority.

(2) The Magistrates Court may vary or cancel a covert surveillance authority on its own initiative or on application made by a worker, employer or other person affected by the authority.

34 Magistrates Court to record details of covert surveillance authority orders

(1) If the Magistrates Court issues, varies or cancels a covert surveillance authority, the court must make and keep a written record of the details of, and reasons for, issuing, varying or cancelling the authority.

(2) The Magistrates Court must take all reasonable steps to protect the confidentiality of a record under this section.

(3) A regulation may prescribe requirements for the following:

(a) the keeping of records in relation to the issue of covert surveillance authorities;

(b) the inspection of the records;

(c) any other matter in relation to the records.

Division 4.3 Restrictions on covert surveillance

35 Offence—conducting covert surveillance other than under covert surveillance authority

(1) An employer commits an offence if the employer conducts covert surveillance of a worker in a workplace.

Maximum penalty: 50 penalty units.

(2) Subsection (1) does not apply if the surveillance is—

(a) conducted in accordance with a covert surveillance authority; or

(b) conducted by a member or officer of a law enforcement agency in the exercise of a function under a territory law or law of another jurisdiction; or

(c) surveillance using an optical surveillance device in a correctional centre or another place where a person is in lawful custody; or

(d) surveillance using an optical surveillance device to monitor operations carried out in a casino in accordance with the *Casino Control Act 2006*; or

(e) surveillance using an optical surveillance device of a legal proceeding or proceeding before a law enforcement agency conducted by a person in the exercise of a function under a territory law or law of another jurisdiction.

Note The employer has an evidential burden in relation to the matters mentioned in s (2) (see Criminal Code, s 58).

36 Defences—surveillance for security of workplaces

(1) It is a defence to a prosecution for an offence against section 35 if the defendant proves that—

(a) covert surveillance was conducted solely to ensure the security of the workplace or people in it (the ***relevant purpose***) and the surveillance of a worker was extrinsic to the relevant purpose; and

(b) there was a real and significant likelihood of the security of the workplace or people in it being jeopardised if covert surveillance was not conducted; and

(c) the employer notified workers (or a body representing a substantial number of the workers) in the workplace in writing of the intended surveillance for the relevant purpose before it was conducted.

Note The defendant has a legal burden in relation to the matters mentioned in s (1) (see Criminal Code, s 59).

(2) A covert surveillance record in relation to a worker that results from the conduct of surveillance mentioned in this section is not admissible in evidence in a proceeding against the worker unless—

(a) for a disciplinary or legal proceeding—the proceeding relates to the security of the workplace or people in the workplace; or

(b) for a legal proceeding—the desirability of admitting the evidence outweighs the undesirability of admitting evidence that has been obtained in the way in which the evidence was obtained.

Division 4.4 Reporting on covert surveillance authority

37 Offence—failure to give covert surveillance report

(1) An employer commits an offence if—

(a) the Magistrates Court issues a covert surveillance authority to the employer; and

(b) the employer fails to give the court a written report setting out the covert surveillance authority information within 30 days after the end of the covert surveillance authority.

Note If a form is approved under the *Court Procedures Act 2004*, s 8 for the report, the form must be used.

Maximum penalty: 20 penalty units.

(2) In this section:

covert surveillance authority information means the following:

(a) the name of any worker (if practicable), or a description of the group or class of workers who were the subject of the covert surveillance;

(b) the period during which the covert surveillance was conducted;

(c) the kind of surveillance device used and the kind of place where the device was installed or used;

(d) whether any surveillance device has been removed and, if not, why not;

(e) the conditions on the covert surveillance authority;

(f) details of any covert surveillance records made as a consequence of the covert surveillance;

(g) any action taken or proposed to be taken in light of the information obtained;

(h) any reason why a worker who was the subject of the surveillance should not be told of the surveillance;

(i) details of any previous use of covert surveillance in relation to the suspected unlawful activity to which the covert surveillance authority applies;

(j) anything else prescribed by regulation.

38 Orders for covert surveillance record

(1) This section applies if an employer gives a report to the Magistrates Court under section 37 in relation to a covert surveillance authority.

(2) The Magistrates Court may make any order in relation to the use and disclosure of a covert surveillance record that the court considers appropriate, including 1 or both of the following:

(a) an order that a covert surveillance record be delivered to the court to be kept in the court's safekeeping or to be dealt with by the court as it considers appropriate;

(b) an order that a stated person or entity be told of the covert surveillance and given access to a covert surveillance record, or part of a covert surveillance record of the surveillance.

(3) The Magistrates Court must make an order under subsection (2) (b) in favour of the worker the subject of the covert surveillance unless satisfied there is a good reason not to.

(4) In considering whether there is a ***good reason*** not to make an order in favour of the worker, the Magistrates Court must consider whether the surveillance was justified or an unnecessary interference with privacy.

Division 4.5 Covert surveillance records

39 Offence—use and disclosure of covert surveillance other than for a relevant purpose

(1) A person commits an offence if the person uses or discloses to someone else surveillance information in a covert surveillance record.

Maximum penalty: 50 penalty units.

(2) Subsection (1) does not apply if the person did not know, and had no reasonable grounds to know, that the surveillance information was, or was part of, a covert surveillance record.

(3) Also, subsection (1) does not apply if the person uses or discloses the information for 1 or more of the following purposes:

(a) use or disclosure under the conditions of the covert surveillance authority or an order of the Magistrates Court under section 38;

(b) use or disclosure for a purpose that is directly or indirectly related to establishing whether or not a worker is engaged in unlawful activity while at work for the employer under the covert surveillance authority;

(c) use or disclosure for a purpose that is directly or indirectly related to a disciplinary or legal proceeding against a worker as a consequence of any alleged unlawful activity while at work for the employer;

(d) use or disclosure for a purpose that is directly or indirectly related to establishing security arrangements or taking other measures to prevent or minimise the opportunity for unlawful activity while at work for the employer of a kind identified by the covert surveillance record to occur while at work for the employer;

(e) use or disclosure that is reasonably believed to be necessary to avoid an imminent risk of death of, or serious injury to, someone or substantial damage to property;

(f) disclosure to a member or officer of a law enforcement agency for use in connection with the detection, investigation or prosecution of an offence;

(g) use by a member or officer of a law enforcement agency for use in connection with the detection, investigation or prosecution of an offence;

(h) use or disclosure for a purpose that is directly or indirectly related to the taking of proceedings for an offence;

(i) use or disclosure for a purpose that is directly or indirectly related to taking any other action under this Act.

(4) Also, if the covert surveillance record results from covert surveillance conducted other than under a covert surveillance authority, subsection (1) does not apply if the person uses or discloses the information for 1 or more of the following purposes:

(a) disclosure to a member or officer of a law enforcement agency for use in connection with the detection, investigation or prosecution of an offence;

(b) use or disclosure for a purpose that is directly or indirectly related to the taking of proceedings for an offence;

(c) use by a member of a law enforcement agency for any purpose in connection with the detection, investigation or prosecution of an offence;

(d) if the covert surveillance was in relation to a worker of a law enforcement agency—

(i) disclosure to a member or officer of a law enforcement agency for use in connection with disciplinary or managerial action or legal proceedings against the worker as a consequence of any alleged misconduct (other than an unlawful activity) or unsatisfactory performance of the worker; or

(ii) use or disclosure for a purpose that is directly or indirectly related to the taking of disciplinary or managerial action or legal proceedings; or

(iii) disclosure to a member or officer of a law enforcement agency for use in connection with the training of law enforcement members or officers.

Note The person has an evidential burden in relation to the matters mentioned in s (2), (3) and (4) (see Criminal Code, s 58).

40 Information inadvertently obtained under covert surveillance authority

(1) This section applies to information that inadvertently or unexpectedly comes to the knowledge of a person as a direct or indirect result of conducting covert surveillance under a covert surveillance authority.

(2) For any determination by a court as to the admissibility of evidence in a criminal proceeding before the court, the information is not considered to have been obtained in contravention of section 35.

(3) Subsection (1) does not apply if the court is of the opinion that the application for the covert surveillance authority was not made in good faith.

Part 5 Prohibited surveillance

41 Offence—surveillance of private areas etc

(1) An employer commits an offence if the employer conducts surveillance of a worker in a prohibited non-work area.

Maximum penalty: 50 penalty units.

(2) In this section:

prohibited non-work area means 1 of the following non-work areas in a workplace:

(a) a toilet facility;

(b) a change room;

(c) a shower or other bathing facility;

(d) a parent or nursing room;

(e) a prayer room;

(f) a sick bay;

(g) a first-aid room;

(h) any other area in a workplace prescribed by regulation.

42 Surveillance of workers not at work

(1) An employer commits an offence if the employer conducts surveillance of a worker if the worker is not in a workplace.

Maximum penalty: 50 penalty units.

(2) Subsection (1) does not apply if—

(a) the employer conducts surveillance of a worker's use of equipment or resources provided by the employer using a data surveillance device; or

(b) the employer conducts surveillance using a tracking device that includes a tracking function that cannot be deactivated; or

(c) the employer is a law enforcement agency.

Note The employer has an evidential burden in relation to the matters mentioned in s (2) (see Criminal Code, s 58).

(3) For subsection (2) (a), equipment or resources are taken to be provided by an employer if the employer has met the cost of the equipment or resources.

43 Use and disclosure of certain tracking device records

A surveillance record in relation to a worker that results from the conduct of surveillance using a tracking device mentioned in section 42 (2) (b) must not be used or disclosed for any purpose.

Part 5A Enforcement

43A The regulator

(1) The regulator has the following functions:

(a) to advise and make recommendations to the Minister and report on the operation and effectiveness of this Act;

(b) to monitor and enforce compliance with this Act;

(c) to provide advice and information on workplace privacy to employers and employees under this Act and to the community;

(d) to conduct and defend proceedings under this Act before a court or tribunal;

(e) any other function given to the regulator by this Act.

Note A reference to an Act includes a reference to statutory instruments made or in force under the Act, including a regulation and any law or instrument applied, adopted or incorporated by the Act (see Legislation Act, s 104).

(2) The regulator has the same powers to obtain information in relation to a possible contravention of this Act or that will assist the regulator to monitor or enforce compliance with this Act that the regulator has under the *Work Health and Safety Act 2011*, section 155 in relation to that Act.

(3) In addition, the regulator has all the powers that an inspector has under this Act.

(4) The regulator may delegate the regulator's powers and functions under this Act to another person.

Note For the making of delegations and the exercise of delegated functions, see the Legislation Act, pt 19.4.

43B Inspectors

An inspector under the *Work Health and Safety Act 2011* is an inspector for this Act.

43C Functions and powers of inspectors

(1) An inspector has the following functions and powers under this Act:

(a) to provide information and advice about compliance with this Act;

(b) to require compliance with this Act through the issuing of notices under the *Work Health and Safety Act 2011*, part 10 (Enforcement measures);

(c) to investigate contraventions of this Act and assist in the prosecution of offences.

(2) The *Work Health and Safety Act 2011*, section 161 (Conditions on inspectors' compliance powers) and section 162 (Inspectors subject to regulator's directions) apply to an inspector in relation to the exercise of a function or power under this Act.

43D Securing compliance

(1) An inspector may exercise powers the inspector has under the following provisions of the *Work Health and Safety Act 2011* for the purpose of securing compliance with this Act:

(a) division 9.3 (Powers relating to entry);

(b) division 9.5 (Other matters).

(2) The following provisions of the *Work Health and Safety Act 2011* apply in relation to any exercise of those functions:

(a) division 9.4 (Damage and compensation);

(b) division 9.6 (Offences in relation to inspectors).

(3) For this section, the provisions of the *Work Health and Safety Act 2011* mentioned in this section apply as if—

(a) a reference in those provisions to a workplace were a reference to a workplace under this Act; and

(b) any other necessary changes were made.

43E Enforcement measures

(1) The *Work Health and Safety Act 2011*, part 10 (Enforcement measures) applies for the purpose of enforcing compliance with this Act.

(2) For this section, the *Work Health and Safety Act 2011*, part 10 applies as if—

(a) a reference in that part to a workplace were a reference to a workplace under this Act; and

(b) a reference to contravening a provision were a reference to contravening a provision of this Act; and

(c) any other necessary changes were made.

Note A reference to an Act includes a reference to statutory instruments made or in force under the Act, including a regulation and any law or instrument applied, adopted or incorporated by the Act (see Legislation Act, s 104).

Part 6 Miscellaneous

44 Offences—security of surveillance records

(1) An employer commits an offence if the employer fails to take reasonable steps to protect surveillance records it holds from misuse, loss, unauthorised access, modification or disclosure.

Maximum penalty: 20 penalty units.

(2) An employer commits an offence if—

(a) a surveillance record is no longer needed for any purpose for which the record may be used or disclosed under this Act; and

(b) the employer fails to take reasonable steps to destroy or permanently de-identify the surveillance record.

Maximum penalty: 20 penalty units.

46 Approved forms

(1) The Executive may, in writing, approve forms for this Act.

(2) If the Executive approves a form for a particular purpose, the approved form must be used for that purpose.

Note For other provisions about forms, see the Legislation Act, s 255.

(3) An approved form is a notifiable instrument.

Note A notifiable instrument must be notified under the Legislation Act.

47 Regulation-making power

The Executive may make regulations for this Act.

Note A regulation must be notified, and presented to the Legislative Assembly, under the Legislation Act.

Dictionary

(see s 3)

Note 1 The Legislation Act contains definitions and other provisions relevant to this Act.

Note 2 For example, the Legislation Act, dict, pt 1, defines the following terms:

- Corporations Act
- correctional centre
- Executive
- exercise
- function
- Magistrates Court
- Minister (see s 162).

adverse action—see the *Fair Work Act 2009* (Cwlth), section 342.

business or undertaking—see section 9.

computer means an electronic device for storing or processing information.

conduct surveillance—see section 11.

covert surveillance—see section 24.

covert surveillance authority, for part 4 (Covert surveillance)—see section 25.

covert surveillance record, for part 4 (Covert surveillance)—see section 25.

data surveillance device—see section 11.

electronic communication means communication by electronic means.

Examples

email, instant messaging

Note An example is part of the Act, is not exhaustive and may extend, but does not limit, the meaning of the provision in which it appears (see Legislation Act, s 126 and s 132).

employer—see section 8.

law enforcement agency—

(a) see the *Spent Convictions Act 2000*, dictionary; and

(b) includes an entity prescribed by regulation.

non-work area means an area in a workplace where a worker is not directly engaged in work.

Examples

tearoom, recreation room

Note An example is part of the Act, is not exhaustive and may extend, but does not limit, the meaning of the provision in which it appears (see Legislation Act, s 126 and s 132).

optical surveillance device—see section 11.

prohibited surveillance means surveillance prohibited under part 5.

regulator—see the *Work Health and Safety Act 2011*, dictionary.

surveillance—

(a) see section 11; or

(b) for part 3 (Notified surveillance)—see section 12.

surveillance device—see section 11.

surveillance information means information obtained, recorded, monitored or observed as a result of surveillance conducted in relation to a worker.

surveillance record means a record or report of surveillance information.

surveillance supervisor, for part 4 (Covert surveillance)—see section 25.

tracking device—see section 11.

unlawful activity, for part 4 (Covert surveillance)—see section 25.

worker—see section 7.

workplace—see section 10.

Endnotes

1 About the endnotes

Amending and modifying laws are annotated in the legislation history and the amendment history. Current modifications are not included in the republished law but are set out in the endnotes.

Not all editorial amendments made under the *Legislation Act 2001*, part 11.3 are annotated in the amendment history. Full details of any amendments can be obtained from the Parliamentary Counsel's Office.

Uncommenced amending laws and expiries are listed in the legislation history and the amendment history. These details are underlined. Uncommenced provisions and amendments are not included in the republished law but are set out in the last endnote.

If all the provisions of the law have been renumbered, a table of renumbered provisions gives details of previous and current numbering.

The endnotes also include a table of earlier republications.

2 Abbreviation key

A = Act
AF = Approved form
am = amended
amdt = amendment
AR = Assembly resolution
ch = chapter
CN = Commencement notice
def = definition
DI = Disallowable instrument
dict = dictionary
disallowed = disallowed by the Legislative Assembly
div = division
exp = expires/expired
Gaz = gazette
hdg = heading
IA = Interpretation Act 1967
ins = inserted/added
LA = Legislation Act 2001
LR = legislation register
LRA = Legislation (Republication) Act 1996
mod = modified/modification
NI = Notifiable instrument
o = order
om = omitted/repealed
ord = ordinance
orig = original
par = paragraph/subparagraph
pres = present
prev = previous
(prev...) = previously
pt = part
r = rule/subrule
reloc = relocated
renum = renumbered
R[X] = Republication No
RI = reissue
s = section/subsection
sch = schedule
sdiv = subdivision
SL = Subordinate law
sub = substituted
underlining = whole or part not commenced or to be expired

3 Legislation history

Workplace Privacy Act 2011 A2011-4

notified LR 24 February 2011
s 1, s 2 commenced 24 February 2011 (LA s 75 (1))
pt 3, pt 4 commenced 24 August 2011 (s 2 (2))
remainder commenced 10 March 2011 (s 2 (1))

as amended by

Workplace Privacy Amendment Act 2016 A2016-22 (as am by A2016-37 sch 1 pt 1.22)

notified LR 14 April 2016
s 1, s 2 commenced 14 April 2016 (LA s 75 (1))
s 5, ss 7-16 commence 14 April 2018 (s 2 (2) (as am by A2016-37 amdt 1.44))
remainder commenced 14 October 2016 (s 2 (1) (as am by A2016-37 amdt 1.44) and LA s 79)

Justice and Community Safety Legislation Amendment Act 2016 A2016-37 sch 1 pt 1.22

s 1, s 2 commenced 22 June 2016 (LA s 75 (1))
amdt 1.45 commences 14 April 2018 (LA s 79A and see Workplace Privacy Amendment Act 2016 A2016-22 s 2 (2) (as am by this Act amdt 1.44))
sch 1 pt 1.22 remainder (amdt 1.44) commenced 29 June 2016 (s 2)

Note This Act only amends the Workplace Privacy Amendment Act 2016 A2016-22.

4 Amendment history

Commencement
s 2 om LA s 89 (4)

Additional requirements for tracking devices
s 17 am A2016-22 s 4

Definitions—pt 4
s 25 def ***unlawful activity*** am A2016-22 s 6

Enforcement
pt 5A hdg ins A2016-22 s 17

The regulator
s 43A ins A2016-22 s 17

Inspectors
s 43B ins A2016-22 s 17

Functions and powers of inspectors
s 43C ins A2016-22 s 17

Securing compliance
s 43D ins A2016-22 s 17

Enforcement measures
s 43E ins A2016-22 s 17

Offences—security of surveillance records
s 44 am A2016-22 s 18

Report on covert surveillance to Legislative Assembly
s 45 om A2016-22 s 19

Review of Act
s 48 exp 10 March 2013 (s 48 (3))

Court Procedures Act 2004
New section 41 (2) (fa)
s 49 om LA s 89 (3)

Dictionary
dict def ***regulator*** ins A2016-22 s 20

5 Earlier republications

Some earlier republications were not numbered. The number in column 1 refers to the publication order.

Since 12 September 2001 every authorised republication has been published in electronic pdf format on the ACT legislation register. A selection of authorised republications have also been published in printed format. These republications are marked with an asterisk (*) in column 1. Electronic and printed versions of an authorised republication are identical.

Republication No and date	Effective	Last amendment made by	Republication for
R1 10 Mar 2011	10 Mar 2011– 23 Aug 2011	not amended	new Act
R2 24 Aug 2011	24 Aug 2011– 10 Mar 2013	not amended	commenced provisions
R3 11 Mar 2013	11 Mar 2013– 13 Oct 2016	not amended	expiry of provision (s 48)