Communities and Justice

Public interest exceptions for ss 11, 12 & 14 of the Surveillance Devices Act 2007

Consultation Outcomes Report

October 2025

NSW GOVERNMENT

Contents

List of Abbreviations

Biosecurity Act	*Biosecurity Act 2015* (NSW)
Crimes Act	*Crimes Act 1900* (NSW)
Cth Privacy Act	*Privacy Act 1998* (Cth)
Corp Act	*Corporations Act 2001* (Cth)
DCJ	Department of Communities and Justice
Health Privacy Act	*Health Records and Information Privacy Act 2002* (NSW)
ICAC	*Independent Commission Against Corruption*
ICAC Act	*Independent Commission Against Corruption Act 1988*
ICAC Committee	Joint Parliamentary Committee on the Independent Commission Against Corruption
illegal surveillance material	Any of the following: • a private conversation, record of an activity, report of a private conversation or an activity, obtained as a result of a use of a listening device, optical surveillance device or tracking device in breach of the SD Act • information about the input of information into or output of information from a computer, obtained as a result of a use of data surveillance device in breach of the SD Act
ILP Act	*Inclosed Lands Protection Act 1901* (NSW)
Investigative body	Any department, agency, authority or organisation that has been given statutory powers under a NSW or Commonwealth law to investigate certain matters, including all law enforcement agencies.
LECC	Law Enforcement Conduct Commission
Model legislation	National model legislation for warrant powers set out in Standing Committee of Attorneys-General and Australasian Police Ministers Council Joint Working Group on National Investigation Powers, *Cross-Border Investigative Powers for Law Enforcement* (Report, November 2003).
NSWPF	New South Wales Police Force
NSW Privacy Act	*Privacy and Personal Information Protection Act 1998* (NSW)
Cth PID Act	Public Interest Disclosures Act 2013 (Cth)
PID Act	*Public Interest Disclosures Act 2022 (NSW)*
SD Act	*Surveillance Devices Act 2007* (NSW)
SD Regulation	*Surveillance Devices Regulation 2022*

Whistleblower protection provisions	Provision in statutes which protect a person against criminal, civil and administrative/disciplinary liability for voluntarily disclosing certain information to certain authorities.

Executive Summary

The *Surveillance Devices Act 2007* (**SD Act**) contains offences for using different types of surveillance devices in certain circumstances. The offences in ss 7, 8, 9 and 10 of the SD Act restrict the use of listening devices, optical surveillance devices, tracking devices and data surveillance devices respectively.

The SD Act also contains offences which restrict the possession, communication and publication of material that has been obtained, directly or indirectly, through using a surveillance device in breach of the Act (**illegal surveillance material**):

- **Section 11** makes it an offence for a person to **publish or communicate** a private conversation, a record of an activity, or a report of a private conversation or an activity if it has come to the person's knowledge as a direct or indirect result of a use of a **listening device, optical surveillance device or tracking device** in breach of ss 7, 8 or 9 of the SD Act.
- **Section 12** makes it an offence for a person to **possess** a record of a private conversation or an activity if the person knows the record has been obtained, directly or indirectly, by use of a **listening device, optical surveillance device or tracking device** in breach of ss 7, 8 or 9 of the SD Act.
- **Section 14** makes it an offence for a person to **publish or communicate** information about the input of information into, or the output of information from, a computer obtained as a direct or indirect result of the use of a **data surveillance device** in breach of s 10 of the SD Act.

While there are exceptions in ss 11, 12 and 14 of the SD Act, those sections do not contain any general exceptions that would permit a report, recording or information that was obtained by illegal use of a surveillance device to be possessed, communicated or published if it is in the public interest.

Chapter 2 of this report provides some background to the SD Act and discussion of the offences in the Act.

Developments in recent years have raised questions as to whether the offences in ss 11, 12 and 14 of the SD Act are too strict. These have included comments from members of the High Court in *Farm Transparency International Ltd v New South Wales*[1], the creation of an exemption from ss 11, 12 and 14 for the Independent Commission Against Corruption, and concerns raised by Members of Parliament during Parliamentary debates. Commentators have noted that the other Australian jurisdictions that have laws which regulate the use of different types of surveillance devices by members of the public include some form of public interest exception for communication and publication of surveillance material obtained. These developments are discussed in **Chapter 3** of this report.

The Department of Communities and Justice (**DCJ**) prepared a Consultation Paper which was published along with a call for submissions on the NSW Government 'Have Your Say' website on 10 April 2024. The consultation was open until 22 May 2024. DCJ also sent the Consultation Paper direct to a number of stakeholders and requested feedback. In the Consultation Paper DCJ asked stakeholders whether public interest exceptions should be inserted into ss 11, 12 and 14 of the SD Act, and if so, what threshold requirements or limitations should be included in the exceptions.

DCJ received 51 submissions from stakeholders. An overview of stakeholders' responses is contained in **Chapter 4** of this report. A clear majority of stakeholders supported some form of public interest exception for ss 11, 12 and 14 being created. The reasons included that such exceptions would allow unlawful and corrupt conduct to be exposed and for evidence of crimes, abuse and cruelty to animals to be provided to and used by appropriate authorities; would protect

[1] (2022) 403 ALR 1.

whistleblowers; and would enable information to be disclosed to influence changes to law and policy on issues of public concern.

In terms of threshold requirements, there was support from a number of stakeholders for a requirement that possession, publication or communication of illegal surveillance material be reasonably necessary in the public interest. The weight of the submissions was against an order from a judge being required to publish or communicate illegal surveillance material, including due to concerns about cost and delay.

The stakeholders were more divided regarding what limitations should apply. Some stakeholders supported communication and publication to and by media organisations. Some stakeholders supported communication and publication to and by any person. Other stakeholders submitted that public interest exceptions should be limited to communication and publication to police, other law enforcement, regulatory enforcement, anti-corruption and integrity bodies.

In terms of what type of material should be able to be communicated or published under a public interest exception, some stakeholders submitted that it should be limited to material about unlawful or corrupt activity, but other stakeholders considered it should not be so confined.

Some stakeholders raised concerns that creating public interest exceptions in ss 11, 12 and 14 of the SD Act would encourage persons to trespass onto private property, particularly premises used for agricultural activities, in order to undertake illegal surveillance.

Chapter 5 of the report examines the protections available under other legislation and common law torts which address concerns raised by some stakeholders about possible negative effects of creating public interest exceptions in ss 11, 12 and 14 of the SD Act. The discussion notes there are a range of laws and torts which protect against invasions of privacy, trespass, interference with the enjoyment of private land and actions which may increase biosecurity risks.

Chapter 5 then discusses the range of NSW and Commonwealth laws which provide protections against criminal liability for whistleblowers who provide certain information to certain authorities. This includes the *Public Interest Disclosures Act 2022* (NSW) and its Commonwealth equivalent, laws supporting the work of integrity agencies such as the *Independent Commission Against Corruption Act 1988*, and laws supporting the work of agencies which address risks to vulnerable persons such as the *Children's Guardian Act 2019*.

That chapter considers how those protections affect the operation of s 11 and s 14 of the SD Act, and considers s 11 and s 14 of the SD Act in light of the offences for concealment of crimes in s 316 and 316A of the *Crimes Act 1900,* which are designed to require persons to disclose information about serious crimes to police.

Chapter 6 contains DCJ's analysis and recommendations for amendments. DCJ concludes there is a need for amendment to ss 11, 12 and 14 to permit illegal surveillance material to be possessed, communicated and published in certain circumstances when such communication and publication would serve the public interest. DCJ recommends amending the offence in s 12 SD Act so that it will only criminalise a person possessing illegal surveillance material if the person was purposefully retaining an unlawful record or was complicit in the illegal use of the surveillance device which generated the material (Recommendation 1).

Given the strong public interest in investigating bodies being able to consider relevant material reflected in the whistleblower protection provisions in other laws, DCJ recommends that exceptions be added to s 11 and s 14 of the SD Act to provide that it will not be an offence under those sections:

- for a person to communicate or publish illegal surveillance material to any investigative body in the public interest (Recommendation 2)
- for an investigative body or prosecuting authority to communicate or publish illegal surveillance material in accordance with its statutory powers and obligations, unless the body or authority was in some way involved in the illegal use of the surveillance device (Recommendation 3).

DCJ proposes that the definition of 'investigative body' should include any department, agency, authority or organisation that has statutory powers under a NSW or Commonwealth law to investigate any matters (included in **Recommendation 2**).

DCJ discusses stakeholder feedback on whether public interest exceptions should be added which allow communication and publication of illegally obtained surveillance material other than to and by investigative bodies, for example, to and by media organisations, or to and by any person. DCJ discusses as an option an exception to s 11 of the SD Act to permit communication or publication of illegal surveillance material to a member of Parliament if it is reasonably necessary in the public interest. DCJ suggests that this option could be considered in the future as part of the statutory review of the amendments proposed in this report (see **Recommendation 5** mentioned below).

DCJ recommends that exceptions should be added to s 11 and s 14 of the SD Act to provide that it will not be an offence under those sections for a person to re-publish illegal surveillance material that has already been published to the world at large, unless the person knows the initial publication was unlawful (**Recommendation 4**).

Finally, DCJ recommends that a statutory review of the amendments should be required five years after the commencement of the amendments proposed in this report (**Recommendation 5**).

The full recommendations are listed in in the next section, and a flow chart illustrating the interaction between the proposed exceptions in Recommendations 1-4 is below on page 8.

DCJ notes that the proposed exceptions will not affect any offences for disclosing certain information under other Acts. If it is an offence under another law to disclose certain information and the information is contained in illegal surveillance device material, the proposed exceptions to s 11 and s 14 of the SD Act will not protect the person from criminal liability under the other law.

1 Recommendations

Recommendation 1 - *Amendment to offence for possession of material in s 12*

Section 12 of the SD Act should be amended so that it is only an offence for a person to possess a record of a private conversation or an activity when:

(a) the person was involved in the record being obtained, directly or indirectly, by use of a listening device, optical surveillance device or tracking device in breach of Part 2 of the SD Act

(b) the person caused a third party to obtain the material by using a device illegally, or

(c) the person knows that the record was obtained through the illegal use of a surveillance device and fails to give the record to an investigative body within a reasonable period of time after becoming aware that the record was obtained illegally

Paragraph (c) should not apply to an officer of an investigative body in possession of a record in connection with the exercise of the investigative body's investigative functions.

Recommendation 2 - *Exceptions to s 11 and s 14 for communication and publication to investigative bodies*

The SD Act should be amended:

(a) To include in s 11 and s 14 of the SD Act an exception that the offences in those sections will not apply to communication or publication to an investigative body that is in the public interest, and to clarify that communication or publication to an investigative body for the purposes of exercising its investigative functions is in the public interest

(b) To include a definition of 'investigative body' that includes any department, agency, authority or organisation that has statutory powers under a NSW or Commonwealth law to investigate any matters.

Recommendation 3 – *Exceptions to s 11 and s 14 for communication and publication by investigative bodies and prosecuting authorities*

Section 11 and section 14 of the SD Act should be amended to include an exception that the offences in those sections will not apply to communication or publication of illegal surveillance material:

- by any person working in an investigative body or a prosecuting authority
- in accordance with their statutory functions and obligations
- to any person (including another investigative body or a prosecuting authority)
- unless the person who communicates or publishes the material knows that a current or former employee of the investigative body or prosecuting authority was involved in the surveillance device being used in breach of the SD Act to obtain the material, including causing another person to use the device illegally.

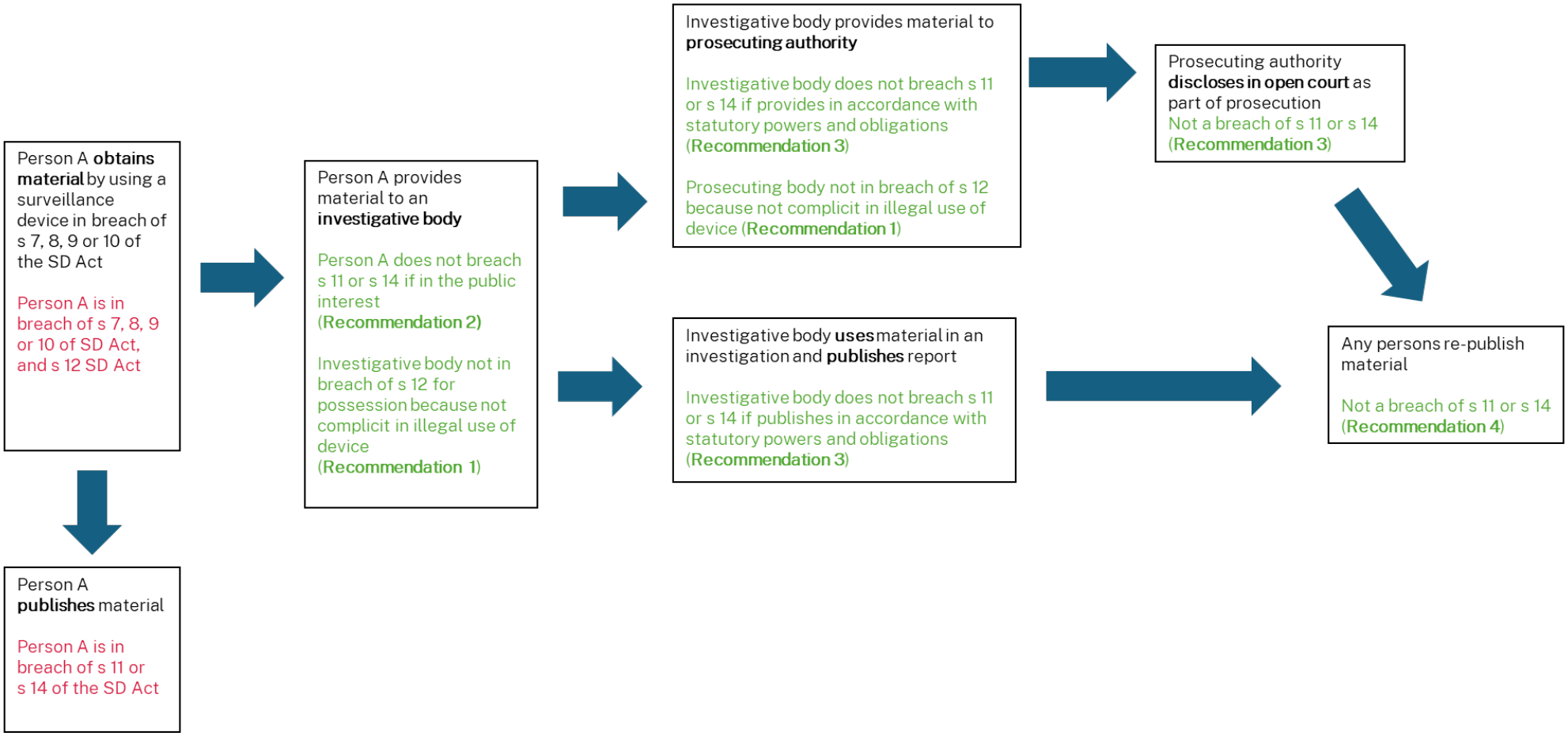
Recommendation 4 – *Exceptions to s 11 and s 14 for re-publication*

Section 11 and s 14 of the SD Act be amended to insert exceptions which provide that it is not an offence under those section for a person (the re-publisher) to communicate or re-publish illegal surveillance device material that another person or body has already been published to the world at large, unless the re-publisher knows the original publication of the material was in breach of s 11 or 14 of the SD Act.

Recommendation 5 – *Requirement for a statutory review 5 years after commencement*

The SD Act be amended to include a requirement that the Minister commence a statutory review of the amendments proposed in this report as soon as practicable after 5 years after the commencement of the amendments.

Flowchart of interaction between proposed amendments to the SD Act



2 The *Surveillance Devices Act 2007*

2.1 Background to the *Surveillance Devices Act 2007*

The SD Act was introduced in 2007 to create a warrant scheme for courts to authorise the NSW Police Force (**NSWPF**) and other specified law enforcement agencies[2] to use surveillance devices on specified premises, vehicles and objects to record conversations and to monitor activities.[3]

The NSW Government largely based the SD Act on national model legislation for warrant powers that was developed in 2003 to enable law enforcement agencies to use surveillance devices in cross-border investigations (**the model legislation**).[4] The SD Act implemented the warrant provisions of the model legislation in relation to both cross-border investigations and investigations contained within NSW.

The focus of the SD Act is on regulating the use of surveillance devices by law enforcement agencies through the warrant scheme. The warrant provisions are contained in Parts 3, 4 and 5 of the SD Act, all of which were based on the model legislation.

The NSW Parliament did not intend for the SD Act to regulate all uses of surveillance devices in NSW. The SD Act was designed to sit alongside other Acts which regulate the use of surveillance devices. This is evident from s 3 of the Act, which states 'this Act is not intended to affect any other law of the State that prohibits or regulates the use of surveillance devices', with a note referring to the *Workplace Surveillance Act 2005*.

2.2 Offences in the *Surveillance Devices Act 2007*

Based on the model legislation, the warrant scheme in the SD Act enabled law enforcement agencies to use listening devices, optical surveillance devices, tracking devices and data surveillance devices. In the Second Reading Speech the Minister for Police explained that that Act would 'assist the operational needs of police by regulating new technology, which is needed to track, monitor and investigate serious crime, and to match the increasingly sophisticated techniques used by criminals'.[5]

Part 2 of the SD Act contains offences which were **not** part of the model legislation. In addition to re-enacting the offence for use of a listening device that was in the *Listening Devices Act 1984* (predecessor to the SD Act), the SD Act created new offences for use of each of the different types of devices which would be available to law enforcement agencies under the warrant scheme. It also created offences for the possession, communication or publication of information obtained from illegally using those devices.

---

[2] The Independent Commission against Corruption, the NSW Crime Commission and the Police Integrity Commission (now its successor the Law Enforcement Conduct Commission).

[3] New South Wales, *Parliamentary Debates,* Legislative Assembly, 6 November 2007, 3578, David Campbell, Minister for Police.

[4] New South Wales, *Parliamentary Debates,* Legislative Assembly, 6 November 2007, 3578, David Campbell, Minister for Police, Standing Committee of Attorneys-General and Australasian Police Ministers Council Joint Working Group on National Investigation Powers, *Cross-Border Investigative Powers for Law Enforcement* (Report, November 2003).

[5] Ibid.

The consent of the Attorney General is required to commence a prosecution against a person for any of the offences in the SD Act, with one limited exception.[6] The Attorney General has delegated the consent function to the NSW Director of Public Prosecutions.[7]

2.2.1 Broad definition of what is a surveillance device

The definition of a surveillance device for the purposes of the SD Act is very broad. It generally includes any instrument, apparatus, equipment or (in the case of data surveillance devices, program) that can be used to:

- overhear, record, monitor or listen to a conversation (referred to as a **listening device**), or
- observe or make a visual record of an activity (referred to as an **optical surveillance device**), or
- determine or monitor the geographic location of a person or object (referred to as a **tracking device**)
- record or monitor the information going in or out of a computer (referred to as a **data surveillance device**).

There are exceptions to these definitions for devices used by people with a disability.

2.2.2 Offences for using surveillance devices

The SD Act contains separate offences for using different types of surveillance devices, as shown in the table below. All of the offences attract a maximum penalty of:

- for a corporation - 500 penalty units ($55,000) (for a corporation)
- for an individual (or non-corporate entity) - 100 penalty units ($11,000) or five years' imprisonment, or both.

Table 1: Offences for use of surveillance devices

Type of device	Scope of the offence for use of the device	Section of the SD Act
Listening devices	Knowingly installing/using/causing to be used/maintaining such a device to: • **overhear, record, monitor or listen** to a **private conversation** to which the person is **not a party**, or • **record** a **private conversation** to which the person **is a party** unless o all the principal parties to the conversation consent to recording, or o one principal party to the conversation consents to recording and the recording ▪ is reasonably necessary for the **protection of the lawful interests** of that principal party, or ▪ is **not made for the purpose of communicating or publishing** the conversation, or a report of the conversation, to persons who are not parties to the conversation.	7

[6] Section 56(1) of the SD Act provides that proceedings for an offence against the Act or the regulations must not be instituted without the written consent of the Attorney General, but sub-s (2) provides that sub-s (1) does not apply to proceedings for a tracking device offence against s 9 where the offence is charged as a domestic violence offence, within the meaning of the *Crimes (Domestic and Personal Violence) Act 2007*.

[7] Attorney General (NSW), 'Director of Public Prosecutions Act 1986 Order' in New South Wales, *Government Gazette of the State of New South Wales*, No 86, 31 August 2012, p 3838-3839.

Type of device	Scope of the offence for use of the device	Section of the SD Act
Optical surveillance devices	Knowingly installing/using/maintaining such a device **on or within premises or a vehicle or on any other object** to visually record or observe the carrying on of an activity if the installation, use or maintenance of the device involves: • **entry onto or into the premises or vehicle without consent** of the owner or occupier, or • **interference with the vehicle or other object without consent** of the person having lawful possession or lawful control of the vehicle or object.	8
Tracking devices	Knowingly installing/using/maintaining a **tracking device to determine the geographical location of—** • a person—**without the consent of that person, or** • an object—**without the consent of a person in lawful possession or having lawful control of that object.**	9
Data surveillance devices	Knowingly installing/using/maintaining such a device **in or in premises** to **record or monitor the input of information into, or the output of information from, a computer on the premises** if the installation, use or maintenance of the device involves— • **entry onto or into the premises without consent** of the owner or occupier of the premises, or • **interference with the computer or a computer network on the premises without consent** of the person having lawful possession or lawful control of the computer or computer network.	10

2.2.2.1 Key limitations of the offences for using listening devices and optical surveillance devices

A key limitation of the offence in s 7 is that it only prohibits recording a conversation if it is a **private conversation**. If a conversation occurs in circumstances in which the parties would reasonably expect that it might be overheard by someone else, it will not be a private conversation (s 4 of the SD Act). For example, if a conversation is occurring in a public space, unless the parties have taken steps to ensure their conversation will not be overheard, it is unlikely that their conversation would be considered private and therefore attract the protection of s 7.

The key limitations of the s 8 offence are that it only prohibits recording the carrying on of an activity if it involves:

- being on or in premises without consent of the owner/occupier
- entering a vehicle without consent of the owner/occupier, or
- interfering with a vehicle or object without consent of the person in lawful possession or control of the vehicle

This means that, for example, if a person uses an optical surveillance device on their own premises, or while on public land, or while on private premises with the permission of the owner or occupier of the premises (for example if the person is employed to work on those premises by the owner or occupier) then generally their use of the device will not be caught by s 8 of the SD Act.

It is also important to note that under s 8 of the SD Act the consent or lack of consent of the person who is being recorded is irrelevant.

2.2.2.2 Exceptions to offences for using surveillance devices

There are exceptions to each of the offences in ss 7-10, but they are different for each. All of those offences have exceptions for the installation, use and maintenance of a surveillance device which is done in accordance with either:

- a warrant issued by a court to a law enforcement officer under Part 3 of the SD Act
- the emergency authorisation provisions available to law enforcement officers in Division 4 of Part 3 of the SD Act, or
- a law of the Commonwealth.

The offence for using a tracking device in s 9 of the SD Act also contains a broad exception permitting installation, use or maintenance of a tracking device for a lawful purpose.

There are also exceptions to ss 7 and 8 which permit police or and other law enforcement officers to use listening devices and optical surveillance devices in specific circumstances. For example, those sections contain exceptions for use of Body-Worn Video cameras by police, or law enforcement officers recording the execution of search warrants.

None of the offences in sections 7-10 for use of surveillance devices contain an exception for use in the public interest. **It is not proposed as part of this consultation that any exceptions be inserted into the offences in ss 7-10 of the SD Act to permit *use of surveillance devices* in the public interest.**

2.2.3 Offences for using surveillance device information or recordings

The SD Act also contains offences for possessing, communicating or publishing information, a report or a recording that was obtained by a person using a surveillance device in breach of ss 7-10 of the Act.

Under s 11 of the SD Act it is an offence for a person to **publish or communicate**:

- a private conversation or a report of a private conversation, or
- a record or report of an activity

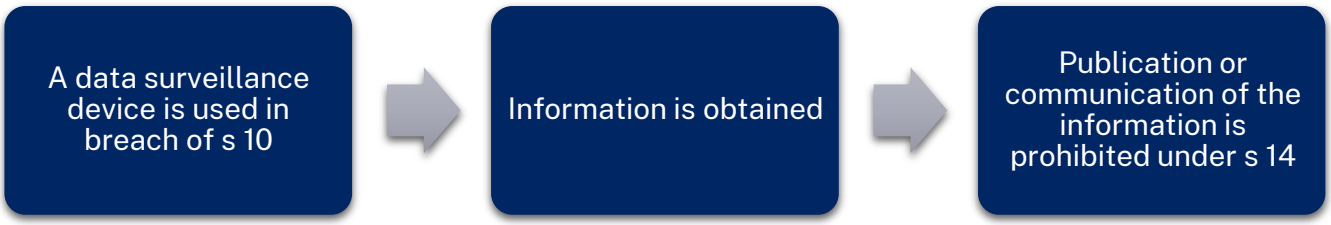
if the conversation, report or record has come to the person's knowledge as a result of the use of a surveillance device in breach of **ss 7, 8 or 9 of the SD Act**.

Section 12 of the SD Act makes it an offence for a person to **possess** a record of a private conversation or an activity if the person knows it has been obtained by a person using a surveillance device in breach of **ss 7, 8 or 9 of the Act**.

Section 14 applies specifically to information obtained from use of a data surveillance device. It provides that a person must not **publish, or communicate** to any person, any information regarding the input of information into, or the output of information from, a computer obtained as a direct or indirect result of the use of a data surveillance device in contravention of **s 10.**

The diagrams below show the relationship between the offences in sections 7-10 of the SD Act, and the offences in ss 11, 12 and 14 of the Act.

Illustration 1: Relationship between the offences in the SD Act



As illustrated above, if the use of a surveillance device did not breach ss 7, 8, 9 or 10 of the SD Act, then possession, communication or publication of the information or record obtained through that use will not breach ss 11, 12 or 14.

2.2.3.1 Exceptions which allow use of information or recordings

There are no general exceptions to the offences in sections 11, 12 and 14 to permit a report, recording or information that was obtained by illegal use of a surveillance device to be possessed, communicated or published if it is in the public interest.

However, there are exceptions in ss 11 and 14 which allow communication or publication that is no more than is reasonably necessary in connection with an imminent threat of:

- serious violence to persons, or
- substantial damage to property, or
- commission of a serious narcotics offence.[8]

Section 12 contains an exception which provides that possessing a record of a private conversation or activity will not breach that section if the record was communicated or published to that person in circumstances that did not contravene s 11.[9]

There are also other limited exceptions, for example, if the record or report of a private conversation or an activity is possessed, communicated or published with the consent of all the main parties to that conversation or activity.[10]

[8] *Surveillance Devices Act 2007* (NSW) s 11(2)(b) and s 14(2)(b).

[9] *Surveillance Devices Act 2007* (NSW) s 12 (2)(c).

[10] *Surveillance Devices Act 2007* (NSW) s 11(2)(a)(ii) and s 12(2)(b).

3 Why we conducted a consultation

In recent years there have been developments which have raised questions as to whether the offences in the SD Act for possession, communication and publication of surveillance device material are too strict.

3.1 *Farm Transparency International Ltd v New South Wales*

In the 2022 case *Farm Transparency International Ltd v New South Wales*[11] the High Court was required to determine a constitutional challenge to the validity of ss 11 and 12 of the SD Act brought on the ground that those sections affect **freedom of communication about political matters**. Farm Transparency argued that ss 11 and 12 of the SD Act infringed on the implied constitutional freedom of political communication because those sections prohibit communication and publication of reports and recordings which may be relevant to public discussion about important political matters, for example animal cruelty.

All Justices of the High Court agreed that the offences in ss 11 and 12 of the SD Act burden the implied constitutional freedom of political communication because they prohibit possession, communication and publication of a record obtained in breach of s 8 of the SD Act. However, all Justices also agreed that the offence in s 8 of the SD Act has the legitimate aim of protecting the privacy of activities that occur on private property, and ss 11 and 12 contribute to that aim.

A majority of the Court concluded that the limits that ss 11 and 12 of the SD Act place on political communication were justifiable in circumstances where:

- the record that was possessed, communicated or published did not reveal unlawful activity, and
- the person who possessed, communicated or published the record was complicit or involved in the breach of s 8 through which the record was obtained.

3.2 Exemption created for the Independent Commission Against Corruption

On 23 August 2023, section 6A was inserted into the *Surveillance Devices Regulation 2022* (**SD Regulation**) to provide that the Independent Commission Against Commission (**ICAC**) is exempt from Part 2 of the SD Act in relation to obtaining, possessing, publishing or communicating, in accordance with the *Independent Commission Against Corruption Act 1988,* material that has been obtained by a third party using a surveillance device in breach of the SD Act (**the ICAC Regulation**).[12]

This exemption was created to support an ongoing investigation by ICAC into alleged corrupt conduct. The exemption does not permit ICAC officers to use a surveillance device in breach of ss 7-10 of the SD Act, and they are only allowed to use the information, records or reports they receive for their work investigating corruption. The exemption is temporary and will expire on 31 December 2025.

On 12 September 2023 the Hon. John Ruddick MLC moved a motion in the Legislative Council to disallow the ICAC Regulation. In opposing that motion the Hon. John Graham, Special Minister of State, Minister for Roads, Minister for the Arts, Minister for Music and the Night-time Economy, and Minister for Jobs and Tourism, stated that the Government was of the view, after considering the advice of the [ICAC] Chief Commissioner, that it was in the public interest for the ICAC to exercise its

[11] (2022) 403 ALR 1.

[12] *Surveillance Devices Amendment (ICAC) Regulation 2023*.

statutory investigative powers, including by using material created by third parties in contravention of the SD Act.[13]

3.3 Questions raised by members of Parliament

In 2018 the Legislative Council Select Committee on Landowner Protection from Unauthorised Filming or Surveillance considered the issue of trespass on agricultural land by animal rights activists and the protections in the SD Act for property rights. The Committee emphasised the 'need for landowners to have the full protection of the law from unauthorised filming or surveillance', but concluded that 'there will continue to be circumstances where genuine whistleblowers will be the only way to expose animal cruelty'.[14] The Committee recommended the former NSW Government consider a public interest exemption in the SD Act for unauthorised filming or surveillance. A Working Group established by the former NSW Government considered these issues in 2019 and 2020 and did not support an amendment to the SD Act to create any public interest exemptions.

On 12 September 2023 the Hon Emma Hurst MLC spoke against the motion to disallow the ICAC Regulation. In doing so she stated that the offences in the SD Act are 'far too restrictive, far too punitive, and are actually preventing systemic issues like corruption and animal cruelty from being exposed'. Ms Hurst commented that:

> The problem for the ICAC arises because, unlike in other States and Territories, the New South Wales Surveillance Devices Act has no public interest exemption for the offences in sections 11 and 12. They are strict criminal offences. There is no scenario where the private conservations or recording of activities obtained from undercover devices can be published, even if it would clearly be in the public interest to do so — for example, to expose corruption. That has a serious chilling effect on investigations of serious criminal misconduct of all kinds. The Surveillance Devices Act is effectively acting as a gagging law for both the media and authorities like the ICAC…
>
> There are many conceivable scenarios where it may be in the public interest to possess or communicate information obtained from an undercover recording. There are serious concerns that the current laws infringe on the implied constitutional freedom of political communication…[15]

On 11 October 2023, Ms Hurst introduced and second read the Surveillance Devices Amendment (Public Interest Exemptions) Bill 2023 in the Legislative Council. Ms Hurst's Bill would create public interest exceptions to ss 11 and 12 of the SD Act. The Bill would provide an exception to s 11 permitting communication or publication of illegally obtained surveillance device material made in the public interest, and an exception to s 12 permitting possession of the material for the purposes of making a communication or publication in the public interest.

3.4 Exceptions in other jurisdictions

The Northern Territory (**NT**), South Australia, Victoria and Western Australia all have laws that contain offences for the use of different types of surveillance devices by members of the public.[16] There are some key differences in the offences in those laws compared with those in the SD Act, for example:

---

[13] New South Wales, *Parliamentary Debates*, Legislative Council, 12 September 2023, 30.

[14] Legislative Council Select Committee on Landowner Protection from Unauthorised Filming or Surveillance, Parliament of New South Wales, *Landowner protection from unauthorised filming or surveillance* (Report, 25 October 2018) 23.

[15] New South Wales, *Parliamentary Debates*, Legislative Council, 12 September 2023, 35.

[16] *Surveillance Devices Act 2007* (NT); *Surveillance Devices Act 2016* (SA); *Surveillance Devices Act 1999* (Vic); *Surveillance Devices Act 1998* (WA). The laws in the Australian Capital Territory, Queensland and Tasmania only contain general offences for the use of listening devices: see *Listening Devices Act 1992* (ACT); *Invasion of Privacy Act 1971* (Qld) and *Listening Devices Act 1991* (Tas).

- The other jurisdictions only prohibit the use of optical surveillance devices to record **private activities**,[17] but s 8 of the SD Act prohibits the recording of any activities if the recording involves entry onto premises without consent of the owner or occupier.
- The communication and publication offences in the other jurisdictions are structured differently to ss 11 and 14 of the SD Act, as they generally prohibit communication or publication of material that has been obtained as a result of a **legal or illegal use** of a surveillance device to record a private conversation or private activity, but then provide exceptions.[18] Sections 11 and 14 of the SD Act **only** prohibit communication or publication of the material if the surveillance device was used contrary to ss 7, 8, 9 or 10 of the SD Act.
- It is not an offence under the laws in the NT, Victoria and South Australia to possess a record obtained from a surveillance device.

New South Wales also has the longest maximum sentence of imprisonment for possessing, communicating or publishing information, reports or records obtained by illegal use of surveillance devices.

The surveillance device laws in the NT, South Australia, Victoria and Western Australia each contain public interest exceptions. However, those laws adopt different approaches in terms of the scope of the exceptions and the role of courts in approving or monitoring the use of surveillance devices or the publication of material in the public interest. The table below shows the different types of public interest exceptions that have been adopted.

Table 2: Types of public interest exceptions in other jurisdictions

Types of public interest exceptions for possession/communication/ publication of information/reports/records from use of surveillance devices	States and territories which have the type of exception
General exception allowing communication and publication that is reasonably necessary in the public interest	Northern Territory, Victoria[19]
Exception allowing communication and publication by an order from a judge if the surveillance device was used in the public interest	Northern Territory, South Australia, Western Australia[20]
Exception allowing publication or communication to police about serious criminal matters	Western Australia[21]
Exception allowing publication or communication by or to media organisations in the public interest	South Australia[22]

[17] *Surveillance Devices Act 2007* (NT) s 12; *Surveillance Devices Act 2016* (SA) s 5; *Surveillance Devices Act 1999* (Vic) s 7; *Surveillance Devices Act 1998* (WA) s 6.

[18] *Surveillance Devices Act 2007* (NT) s 15; *Surveillance Devices Act 2016* (SA) ss 9-10 and s 11; *Surveillance Devices Act 1999* (Vic) s 11 and 12; *Surveillance Devices Act 1998* (WA) s 9.

[19] *Surveillance Devices Act 2007* (NT) s 15(2)(b)(i); *Surveillance Devices Act 1999* (Vic) s 11(2)(b)(i).

[20] *Surveillance Devices Act 2007* (NT) s 46; *Surveillance Devices Act 2016* (SA) s 11; *Surveillance Devices Act 1998* (WA) s 31.

[21] *Surveillance Devices Act 1998* (WA) s 9(2)(b).

[22] *Surveillance Devices Act 2016* (SA) s 10(2).

4 Overview of stakeholder submissions

In response to its call for submissions on the review, DCJ received 51 submissions, including

- 32 submissions from institutions or organisations
- 19 submissions from individuals, including 1 campaign submission which was substantively re-submitted by 144 persons in New South Wales.[23]

DCJ has considered all of the submissions it received.

4.1 Creating public interest exceptions

The vast majority of submissions supported inserting public interest exceptions into ss 11, 12 and 14 of the SDA to allow information, records and reports obtained from using a surveillance device in breach of the Act to be communicated, published or possessed if it is in the public interest for the following reasons:

- to expose unlawful and corrupt conduct;
- to allow evidence of crimes, sexual violence, domestic violence, abuse of a child or a person with disability, or cruelty or mistreatment of animals to be provided to police or other appropriate authorities
- to promote transparency and accountability and enable an open democratic society;
- to remove the chilling effect the SD Act currently has on whistleblowers, media organisations and enforcement agencies;
- to drive meaningful reforms and improvements to issues of public concern;
- to balance the public interest with protecting individuals' privacy;
- to assist investigative agencies with their functions under their relevant Acts; and
- the need for consistency with the other Australian jurisdictions.

A small number of submissions opposed inserting public interest exceptions into ss 11, 12 and 14 of the SDA to allow information, records and reports obtained from using a surveillance device in breach of the Act to be communicated, published or possessed if it is in the public interest for the following reasons:

- potential damage to agricultural production and processing facilities;
- distress for individual farmers, processors and their staff;
- concerned about people's right to privacy and the exposure of people's personal details;
- encourage activist groups to engage in illegal trespass to capture footage; and
- trespassers ignoring biosecurity protocols and potential spread of diseases.

4.2 Threshold requirements for a public interest test

[23] The same campaign submission was also substantively re-submitted by 466 persons residing outside of New South Wales, mostly persons residing in other countries.

4.2.1 Reasonably necessary

Some submissions supported including a requirement that the possession, communication or publication be reasonably necessary in the public interest. Some submissions considered that the exception should be drafted closer to Victoria's surveillance device legislation which allows a communication or publication 'that is no more than is reasonably necessary in the public interest'. These submissions considered that the Victorian model is working well. A stakeholder submission highlighted that such a requirement would be consistent with the requirement in section 19(1)(a) of the SDA that an eligible judge be satisfied that there are reasonable grounds for the suspicion or belief founding an application for a surveillance device warrant.

Some submissions suggested that there should be clear guidelines and examples to assist with interpretation of what is reasonably necessary and in the public interest.

Some submissions recommended including a definition of 'public interest' in the SD Act that is broad to include a range of societal issues. These submissions noted that a non-exhaustive definition is provided in the surveillance device legislation of Western Australia and the Northern Territory.

Some submissions raised concerns that the reasonably necessary requirement would add complexity to the legislation as it would be necessary to interpret the requirement and determine the scope on a case-by-case basis resulting in additional work for the courts. Further, a stakeholder submission highlighted that the interpretation of reasonable may change over time as specific issues become the target of the public's interest, which introduces an extreme level of uncertainty about the consistency and reliability of the established common law.

4.2.2 Belief on reasonable grounds

Some submissions supported including a requirement that the person believes on reasonable grounds that possessing, communicating or publishing the information, record or report is in the public interest. These submissions considered that this requirement is already well established in the courts and will limit to situations where the use of a surveillance device is done in good faith. Further, the submissions recommended that there should be a robust process for reviewing and challenging the determination of 'reasonable grounds' such as a mechanism of appeal to an independent body or to the courts.

Some submissions opposed the belief on reasonable grounds requirement as considered that it may result in defendants attempting to justify their use of surveillance devices based on their own subjective views of what is in the public interest. A stakeholder submission raised concerns about how an exception which has a subjective component would work with a requirement that the conduct is 'reasonably necessary' in the public interest.

4.2.3 An order from a judge

Most submissions were against including a requirement for an order from a judge to permit the information, report or record to be communicated or published in the public interest. Stakeholders considered that requiring an order from a judge would be onerous, time consuming and may cause delays in preventing any harm or abuse. For example, one stakeholder submitted that:

> Such a requirement places an unnecessary burden (of cost, time, and resources more broadly) on the relevant court as well as prospective parties... [and] would effectively operate as a de facto injunction on the publication of such material.

Some submissions highlighted that such a requirement may deter individuals from coming forward with surveillance device material and present an unreasonable barrier to parties communicating to investigative agencies.

Some submissions supported including a judge order requirement as considered that it adds an extra layer of scrutiny and protection against misuse. A stakeholder submission raised concerns about how this requirement would work in practice such as which court would have jurisdiction, avenues for appeal and resourcing implications for all relevant stakeholders.

4.3 Limits on the communication or publication of information or records in the public interest

4.3.1 By and to any person

Some submissions supported the exceptions allowing possession, communication and publication by and to any person if it is in the public interest. These submissions considered that given the broad range of individuals who may need to rely on the exceptions such a limit is appropriate.

Some submissions submitted that this limit is too broad, and the exceptions should only allow possession, communication and publication to investigative agencies if it is in the public interest. A stakeholder submission raised concerns that introducing exceptions that permit possession, communication and publication by or to any person may cause unauthorised surveillance to gather and publish information for personal and political gain rather than for genuine public interest matters.

4.3.2 Unlawful and/or corrupt activity

Some submissions argued that the exceptions should only allow communication and publication about unlawful or corrupt activity in the public interest. Some submissions suggested that abuse of vulnerable persons should also be included. Some submissions highlighted that there may be conduct that is not illegal but is unethical and of public concern and once exposed, reforms are then implemented to make that conduct illegal.

4.3.3 Law enforcement, regulatory, anti-corruption and integrity bodies

A majority of stakeholder submissions supported exceptions that permitted communication and publication to police, other law enforcement agencies, regulatory enforcement agencies, anti-corruption and integrity bodies.

Some submissions supported communication and publication being limited to police, other law enforcement, regulatory enforcement, anti-corruption and integrity bodies. A stakeholder submission suggested that the exceptions should be limited to communication and publication with investigative agencies noting this terminology is used in privacy legislation. Further, a stakeholder submission suggested that there should also be limitations imposed on who can communicate to enforcement agencies. The submission considered that the limit may inadvertently allow officers of law enforcement agencies to bypass the warrant scheme in the SD Act by making unlawful recordings that they believe are necessary to their investigations without a surveillance warrant by justifying their conduct as being in the public interest.

4.3.4 Media organisations

Some submissions supported the exceptions allowing communication and publication to and by media organisations in the public interest. These submissions referred to the benefits of including media organisations in the limits due to media organisations publishing sensitive topics, exposing wrongdoing, and supporting whistleblowers. A stakeholder submission noted that there may be circumstances where communication and publication to media organisations should not be allowed such as cases involving National Disability Insurance Scheme participants given that they are a vulnerable group.

Some submissions were against allowing communication and publication to and by media organisations as considered that it may encourage illegal activity and trespass, and it is difficult to regulate the media. A stakeholder submission raised that the *Public Interest Disclosures Act 2022* (NSW) provides for circumstances in which serious wrongdoing in or affecting the public sector can be disclosed to the media under the statutory protections. Other whistleblower protections may apply under the *Corporations Act 2001* (NSW) that may cover corporate wrongdoing. The submission

also considered that creating an additional exception specifically for media organisations would encroach inappropriately on the objects of the SD Act, specifically section 2A(c).

5 Protections under other laws

5.1 Laws that protect privacy and private property and support biosecurity

A common concern in the few submissions that opposed the creation of public interest exceptions for ss 11, 12 and 14 of the SD Act was that inserting such exceptions would encourage persons to trespass onto private property, particularly premises used for agricultural activities, in order to make recordings. Those submissions raised concerns that such trespass would result in breaches of privacy, damage to property, biosecurity risks and distress for those working on the premises.

DCJ emphasises that there is no intention to create public interest exceptions to the offences in ss 7-10 of the SD Act for use of surveillance devices. Any persons who trespass onto property to record footage will be in breach of s 8 of the SD Act and liable to up to 5 years' imprisonment.

Also, as mentioned above, the key purpose of the SD Act is to authorise and regulate the use of surveillance devices by law enforcement agencies through the warrant scheme in Part 3 of the Act. The SD Act sits alongside other legislation and common law torts which have the primary purpose of protecting privacy, protecting against trespass and interference with the enjoyment of private land and protecting against biosecurity risks, discussed below. It is important for the provisions in the SD Act to be considered in the context of these other laws.

5.1.1 Privacy legislation and new statutory tort for serious invasions of privacy

There are three laws which primarily protect the privacy of persons in NSW, each of which impose duties in relation to the collection, use and disclosure of personal information:

- the *Privacy Act 1988* (Cth) (**Cth Privacy Act**) – which imposes duties on:
  - Australian Government agencies
  - private organisations (including corporations and sole traders) with an annual turnover of more than $3 million, and
  - certain small business operators (referred to as '**APP entities**').
- the *Privacy and Personal Information Protection Act 1998* (**NSW Privacy Act) -** which imposes duties on NSW public sector agencies
- the *Health Records and Information Privacy Act 2002* (**Health Privacy Act**) – which imposes duties on all NSW public sector agencies, private sector persons and corporations (with an annual turnover of more than $3 million) that collect, hold or use health information.

The obligations that each of these Acts impose, and exceptions to those obligations for certain bodies that carry out law enforcement or investigative functions, are discussed in Appendix A.

Until recently, none of these laws currently place obligations on individuals acting in a personal capacity. However, on 10 June 2025 changes to Commonwealth Privacy legislation came into force, including changes to schedule 2 of the Cth Privacy Act. Schedule 2 of the Cth Privacy Act provides for a statutory tort for serious invasions of privacy. An individual may bring an action in court to seek damages and other remedies, with the elements of the tort being:

(1) another person (the defendant) invaded the plaintiff's privacy by **intruding upon the plaintiff's seclusion**, and/or **misusing information** that relates to the plaintiff; and

(2) a person in the position of the plaintiff would have had a **reasonable expectation of privacy** in all of the circumstances; and

(3) the invasion of privacy was **intentional** or **reckless**; and **serious,** and

(4) the public interest in the **plaintiff's privacy outweighed any countervailing public interest**.

The plaintiff does not need to prove that any damage resulted from the invasion of privacy to bring an action. However, the damage or harm a plaintiff suffers will be a relevant factor when assessing the seriousness of the invasion, and the remedies that may be awarded.

The Cth Privacy Act specifies a non-exhaustive list of matters that may constitute **countervailing public interests** for the purposes of element (4) above, which includes:

- freedom of expression, including political communication and artistic expression;
- freedom of the media;
- the proper administration of government;
- open justice;
- public health and safety;
- national security;
- the prevention and detection of crime and fraud.

There are a range of defences and exemptions from liability. For example it is a defence to the cause of action if the invasion of privacy was required or authorised by or under an Australian law or court/tribunal order; or the defendant reasonably believed that the invasion of privacy was necessary to prevent or lessen a serious threat to the life, health or safety of a person; or the invasion of privacy was incidental to the exercise of a lawful right of defence of persons or property, and proportionate, necessary and reasonable. There is also a defence to the action for publishing information if the defendant would be able to establish a defence under a relevant defamation law.

There are exemptions from liability for persons under 18 years of age; collection, preparation and publication of journalistic material by journalists and people who employ or assist journalists; for law enforcement bodies and intelligence agencies and agencies or State or Territory authorities acting in good faith in the performance of their functions or exercise of their powers.

5.1.2 Laws that protect private property

There are a range of offences in NSW that protect property against trespass and damage.

5.1.2.1 Inclosed Lands Protection Act 1901

The *Inclosed Lands Protection Act 1901* (**ILP Act**) contains offences to protect 'inclosed lands' from intrusion and trespass. 'Inclosed lands' include any land enclosed or surrounded by any fence or wall (including natural features such as a river or cliff) marking the boundary, as well as certain prescribed premises.

Section 4 of the ILP Act makes it an offence for a person, without lawful excuse, to enter into inclosed lands without the consent of the owner, occupier or person apparently in charge of those lands, or remain on those lands after being requested by the owner, occupier or person apparently in charge of those lands to leave those lands. The offence is punishable by up to 10 penalty units if the lands are occupied or used in connection with a school, childcare service, hospital or nursing home, and up to 5 penalty units in any other case.

Section 4B of the ILP Act contains aggravated versions of the s 4 offence which apply if the inclosed lands the person entered or remained on are lands on which a business or undertaking is conducted and certain further circumstances are established, for example while on those lands the person:

- interferes with, or attempts or intends to interfere with, the conduct of the business or undertaking, or

- does anything that gives rise to a serious risk to the safety of the person or any other person on those lands, or
- introduces or increases a risk of a biosecurity impact (within the meaning of the *Biosecurity Act 2015*) for those inclosed lands, or
- damages property on agricultural land, or
- wilfully or negligently releases any livestock.

The maximum penalty for the offences under s 4B is 50 penalty units if the offence occurs on land other than agricultural land. If the offence occurs on agricultural land, the maximum penalty is significantly increased to:

- 200 penalty units and/or 3 years' imprisonment if the offender:
  - was accompanied by 2 or more persons when the offence occurred, or
  - does anything that gives rise to a serious risk to the safety of the person or any other person on the lands (i.e. s 4B(1)(b) applies)
- 120 penalty units and/or 12 months' imprisonment in any other case.

It is also an offence under s 4C of the ILP Act, punishable by up to 100 penalty units and/or 12 months' imprisonment, for a person to direct, incite, counsel, procure, commission or induce the commission, on agricultural land, of an offence against section 4B.

One stakeholder in their submission raised a question how any public interest exceptions for the SD Act would operate with the ILP Act, noting that a hospital may set conditions of entry which includes no filming or recording on hospital premises. Public interest exceptions in the SD Act will not affect the operation of the ILP Act, and therefore will not alter the right of owners or occupiers to set conditions on rights of entry.

5.1.2.2 Offences in the *Crimes Act 1900*

There are offences in the *Crimes Act 1900* (Crimes Act) for destroying or damaging property and breaking into houses.

Under s 195 of the Crimes Act it is an offence to intentionally or recklessly destroy or damage another person's property. The maximum penalty for the base offence is 5 years' imprisonment, but the penalty increases if aggravating circumstances are present, in which case the maximum penalty can extend up to 12 years' imprisonment.

There are also offences in Part 4AD of the Crimes Act for destroying or damaging property with the intention of endangering the life of another or causing bodily injury, for threatening to damage or destroy property, and being in possession of explosives or other articles with the intention of using them to destroy or damage property.

Division 4 of Part 4 of the Crimes Act contains offences for breaking into houses. Division 4 contains various offences relating to entering a dwelling-house with the intention to commit a serious indictable offence or entering and committing such an offence. The maximum penalties for the offences range from 10 years' imprisonment up to 25 years' imprisonment (if the person breaks and enters a dwelling house and assaults a person with the intention or murdering or inflicting grievous bodily harm).

5.1.3 Torts of trespass and nuisance

The common law torts of trespass and nuisance also protect against interference with private property, and with the enjoyment of that property.

A person can bring an action for damages against a person for trespass if the latter directly interferes, either intentionally or negligently, with the first person's possession of land without that

person's consent or other lawful authority[24]. There is no need to prove that the interference caused any damage to establish the tort.[25]

A person can bring an action against a person for 'nuisance' if the latter unlawfully interferes with the first person's use or enjoyment of land that that first person owns or occupies.[26] To give rise to a legally actionable nuisance, the interference must be substantial and unreasonable.[27]

5.1.4 *Biosecurity Act 2015*

A number of stakeholder submissions raised questions about how the SD Act interacts with the *Biosecurity Act 2015* (NSW) (**Biosecurity Act**).

The Biosecurity Act provides a framework for preventing, eliminating and minimising biosecurity risks, including pests, diseases, contaminants and other biosecurity matters that are economically significant for primary production industries.

The Biosecurity Act imposes duties in relation to managing biosecurity risks and contains offences for breaching those duties. Section 22 of the Biosecurity Act contains the general biosecurity duty and provides that any person who deals with biosecurity matter (or a carrier of that matter) and who knows, or ought reasonably to know, the biosecurity risk posed or likely to be posed by those actions has a biosecurity duty to ensure that, so far as is reasonably practicable, the biosecurity risk is prevented, eliminated or minimised.

Section 12 of the Biosecurity Act defines 'deals' for the purpose of s 22 as including moving biosecurity matter or a carrier or releasing biosecurity matter or a carrier from captivity.

Section 24 of the Biosecurity Act provides that a breach of a 'mandatory measure' specified in the regulations by a person who deals with biosecurity matter is taken to be a breach of the duty in s 22. Under the *Biosecurity Regulation 2017* compliance with any biosecurity management plan in place at a premises is a mandatory measure.[28] A biosecurity management plan can, for example, restrict how and where persons can enter a place.

It is an offence under s 23 of the Biosecurity Act for a person to fail to discharge their duty under s 22. The offence is punishable by penalties up to:

- $1.1 million and/or 3 years' imprisonment for an individual and $2.2 million for a corporation if the failure was intention or reckless, and the failure caused or was likely to cause a serious biosecurity impact;[29]
- $1.1 million for an individual and $2.2 million for corporations if the offence is committed negligently[30]
- $220,000 for an individual and $440,000 for a corporation in any other case.[31]

Any public interest exceptions to ss 11, 12 and 14 of the SD Act will not affect the duties that apply to persons who deal with biosecurity matter under the Biosecurity Act.

5.2 Laws relating to whistleblowers

[24] *Brown v Tasmania* (2017) 261 CLR 328, 451 [383].

[25] *Plenty v Dillon* (1991) 171 CLR 635, 654–655.

[26] Hargrave v Goldman (1963) 110 CLR 40, 59.

[27] *Hunt Leather Pty Ltd v Transport for NSW* [2023] NSWSC 840, [600].

[28] *Biosecurity Regulation 2017*, s 44C.

[29] *Biosecurity Act 2015* (NSW) s 23(2) and s 279.

[30] *Biosecurity Act 2015* (NSW) s 23(3) and s 280(2).

[31] *Biosecurity Act 2015*, s 23(3) and s 280(1).

A number of submissions raised the issue of whistleblowers. Some submitted that the SD Act should contain comprehensive exceptions or protections for whistleblowers. One stakeholder pointed out that there are already protections for whistleblowers under other legislation such as the *Public Interest Disclosures Act 2022* and the *Corporations Act 2001*. The stakeholder submitted this reduced the need for a public interest exception in the SD Act to allow communication and publication to and by media.

There are a range of existing protections and laws relating to whistleblowers, including:

- protections for NSW public officials under the *Public Interest Disclosures Act 2022* (NSW);
- protections for federal public officials under the *Public Interest Disclosures Act 2013* (Cth);
- protections for corporate whistleblowers under the *Corporations Act 2001* (Cth);
- protections for whistleblowing by members of the public to certain authorities under a number of NSW and Commonwealth Acts, and
- criminal liability for **failing** to report information about a serious indictable offence to police under s 316 and 316A of the Crimes Act.

Each of these are discussed below.

5.2.1 NSW Public officials - *Public Interest Disclosures Act 2022* (NSW)

The *Public Interest Disclosures Act 2022* (**PID Act**) provides a framework for public officials working in the NSW public service to report serious wrongdoing in the NSW public sector and contains certain protections for those who make such reports.

There are three types of public interest disclosures (**PIDs**) that can be made under the PID Act: voluntary PIDs, mandatory PIDs and witness PIDs. For the purposes of this consultation the provisions for voluntary PIDs are the most relevant.

5.2.1.1 What will constitute a voluntary public interest disclosure

Under the PID Act a disclosure of information will meet the definition of a voluntary PID and attract the protections in the PID Act if:

- The disclosure is **made by a public official** (but that includes contractors, sub-contractors and volunteers providing services or exercising functions on behalf of an agency),[32]
- The public official honestly, and on reasonable grounds, believes that the **information shows or tends to show serious wrongdoing**.[33] Serious wrongdoing means one or more of corrupt conduct,[34] serious maladministration,[35] a government information contravention,[36] a local

[32] *Public Interest Disclosure Act 2022*, s 25.

[33] *Public Interest Disclosure Act 2022,* s 26(1).

[34] Corrupt conduct in the PID Act has the same meaning as in the *Independent Commission Against Corruption Act 1988*: PID Act, sch 2.

[35] Serious maladministration is defined as conduct, other than conduct of a trivial nature, of an agency or a public official relating to a matter of administration that is—

(a) unlawful, or

(b) unreasonable, unjust, oppressive or improperly discriminatory, or

(c) based wholly or partly on improper motives: PID Act, sch 2.

[36] A government information contravention means a failure (but not a trivial failure) to comply with the *Government Information (Information Commissioner) Act 2009, Government Information (Public Access) Act 2009*, or *State Records Act 1998*: PID Act, sch 2.

government pecuniary interest contravention,[37] a privacy contravention[38] or a serious and substantial waste of public money.

- The disclosure is **made to** the person's manager, the head of disclosure officer of any NSW public agency, or a Minister or Minister's office (if in writing).[39]

A voluntary PID can also be **made to a journalist or Member of Parliament**, but only if the following additional requirements are also satisfied:

- the disclosure is **substantially true**
- the person who made the disclosure **previously made substantially the same voluntary disclosure** (the previous disclosure) to one of the other types of recipients mentioned above, not on an anonymous basis, and either:
    - did not receive required information[40] from an agency about its handling of the previous disclosure within 6 months after making that disclosure, or
    - received notification from an agency that it decided not to investigate or refer the previous disclosure, or had ceased to investigate the previous disclosure without completing its investigation or referring the matter.[41]

5.2.1.2 Protections from prosecution and detrimental action

If a disclosure by a public official meets the requirements for a voluntary PID, the public official will be given certain protections under the PID Act, including protection from civil and criminal liability for making the disclosure, and protections from detrimental action being taken against them.

Under s 40 of the PID Act a person who makes a voluntary PID has **immunity from civil and criminal liability for making the disclosure**, and is also not liable to disciplinary action for making the disclosure. Section 40 does not confer immunity on the person for past conduct that the person has engaged in, which the person discloses as part of making a PID. However, under s 41 the Attorney General may give an undertaking that the disclosure of past conduct will not be used in evidence against the person in civil or criminal proceedings.

The PID Act also includes provisions to protect the person who makes a PID from 'detrimental action' such as bullying, harassment or dismissal as a result of making the PID. These include:

- It is a criminal offence, punishable by up to 200 penalty units or 5 years' imprisonment, or both, to take detrimental action against a person based on a suspicion, belief or awareness that a person has made, may have made or may make a PID (PID Act s 33).
- A person who has been the subject of detrimental action can bring a civil action for damages (PID Act s 35).
- The Supreme Court can grant an injunction where detrimental action is threatened or has occurred (for example, an order to prevent dismissal or to require reinstatement) (PID Act s 37).

---

[37] A local government pecuniary interest contravention means the contravention of an obligation imposed in connection with a pecuniary interest by the Local Government Act 1993 or a code of conduct adopted by a council under the Local Government Act 1993: PID Act, sch 2.

[38] A privacy contravention means a failure, other than a trivial failure, by an agency or public official to comply with the *Privacy and Personal Information Protection Act 1998*, or the *Health Records and Information Privacy Act 2002*: PID Act, sch 2.

[39] *Public Interest Disclosures Act 2022,* s 27.

[40] See s 59 of the *Public Interest Disclosures Act 2022* for what information an agency is required to provide.

[41] *Public Interest Disclosures Act 2022,* ss 27 and 28.

5.2.2 Federal public officials - *Public Interest Disclosures Act 2013* (Cth)

There is a similar regime for public interest disclosures by public officials working at the Federal level under the *Public Interest Disclosures Act 2013* (Cth) (**Cth PID Act**). Under the Cth PID Act persons employed by the Australian Government or Commonwealth companies, agencies or authorities, or service providers with contracts with the Commonwealth, can disclose information they believe on reasonable grounds tends to show 'disclosable conduct' by a Commonwealth agency, public official or a contracted Commonwealth service provider. The categories of disclosable conduct are generally similar to those under the NSW PID Act, however they also include:

- any conduct that contravenes a law of the Commonwealth or a State or Territory
- conduct that unreasonably results in or increases a risk of danger to the health or safety of one or more persons
- conduct that results in or increases a risk of danger to the environment.[42]

The Cth PID Act provides for both 'internal' and 'external' disclosures of information about disclosable conduct. A public official may make an external disclosure to any person (other than a foreign public official) if:

- the public official previously disclosed the information to a Commonwealth agency (an internal disclosure) and
- the relevant agency conducted an investigation of the internal disclosure but either:
  - the public official believes on reasonable grounds:
    - the investigation was inadequate, or
    - the response to that investigation was inadequate, or
  - the investigation was not completed within the time limit in s 52 of the Act,

    and
- the disclosure is **not, on balance, contrary to the public interest**, and
- no more information is publicly disclosed than is **reasonably necessary** to identify one or more instances of disclosable conduct, and
- the information does not consist of, or include, intelligence information, and none of the conduct with which the disclosure is concerned relates to an intelligence agency.[43]

The Cth PID Act contains similar protections for disclosers as the NSW PID Act, namely immunity from criminal, civil and administrative liability for making the disclosure,[44] criminal penalties for reprisal behaviour against the discloser and for disclosing the identity of a discloser,[45] and civil remedies for reprisal behaviour.[46]

5.2.3 Corporate whistleblowers - *Corporations Act 2001* (Cth)

The *Corporations Act 2001* (Cth) (**Corp Act**) contains legal rights and protections for persons who report potential misconduct or breaches of the law by a company, bank, insurance provider and unincorporated associations and body corporates that are trading or financial corporations.

---

[42] *Public Interest Disclosures Act 2013* (Cth), s 29.

[43] *Public Interest Disclosures Act 2013* (Cth), s 26.

[44] *Public Interest Disclosures Act 2013* (Cth), s 10.

[45] *Public Interest Disclosures Act 2013* (Cth), s 19 and s 20.

[46] *Public Interest Disclosures Act 2013* (Cth), ss 14-16.

To attract the protections in the Corp Act the person must qualify as an 'eligible whistleblower'. Generally this includes persons who have a connection to a company or organisation regulated by the Corp Act, such as employees, officers, or persons who have supplied goods or services to a regulated entity.[47] An eligible whistleblower can make a disclosure about misconduct by a regulated entity, an 'improper state of affairs or circumstances' in relation to a regulated entity, or conduct that constitutes an offence under the Corp Act or other financial regulatory legislation or an offence under a Commonwealth law that is punishable by at least 12 months' imprisonment.[48]

An eligible whistleblower must make their disclosure either internally to certain persons in the company or organisation the subject of the disclosure,[49] or externally to the Australian Securities and Investments Commission (**ASIC**) or the Australian Prudential Regulation Authority (**APRA**).[50]

The protections in the Corp Act can also apply if a person makes a whistleblower report to a journalist or an MP in the Commonwealth Parliament or a State or Territory Parliament (referred to as a 'public interest disclosure'). However, similar to under the NSW PID Act, there are additional requirements that must be satisfied for a discloser to be protected for disclosing to such persons. These requirements are:

- the discloser must have previously made a disclosure of the same information to ASIC or APRA;
- at least 90 days must have passed since the discloser made the previous report, the discloser does not have reasonable grounds to believe that action is being, or has been, taken to address the matters to which the previous disclosure related; and after those 90 days the discloser gave ASIC or APRA written notice which identifies the earlier report and states the discloser's intention to make a public interest disclosure, and
- the discloser must have **reasonable grounds to believe** that making a further disclosure to a journalist of MP would **be in the public interest**;
- the extent of the information disclosed to the journalist or MP is 'no greater than is necessary to inform the recipient' about the relevant conduct.[51]

The Corp Act also provides protections for 'emergency disclosures' to journalist and MPs in relation to information concerning 'a substantial and imminent danger to the health or safety of one or more persons or to the natural environment', with similar requirements as for public interest disclosures.[52]

Like the Cth and NSW PID Acts, the Corp Act provides that a person who makes a disclosure that qualifies for protection under that Act is not subject to any civil, criminal or administrative liability (including disciplinary action) for making the disclosure.[53] The Corp Act also contains criminal offences and civil penalties for detrimental action against a person for making a disclosure that attracts the protection of the Act.[54]

5.2.4 Whistleblowing by members of the public

There are a range of NSW and Commonwealth Acts which provide protections to members of the public who disclose information about misconduct or wrongdoing to certain authorities that have statutory investigative powers.

---

[47] *Corporations Act 2001* (Cth), s 1317AAA.

[48] *Corporations Act 2001* (Cth), s 137AA(4) and (5).

[49] See *Corporations Act 2001* (Cth) s 1317AAC(1)(a)-(d).

[50] *Corporations Act 2001* (Cth), s 1317AAA(1)(b).

[51] *Corporations Act 2001* (Cth), s 1317AAD(1).

[52] *Corporations Act 2001* (Cth), s 1317AAD(2).

[53] *Corporations Act 2001* (Cth), s 1317AB(1).

[54] *Corporations Act 2001* (Cth), s 1317AC -1317AF (and s 1311(1)).

For example when the NSW PID Act commenced in 2023 it increased protections for members of the public who disclose misconduct or wrongdoing to the ICAC, the NSW Ombudsman and the New South Wales Law Enforcement Conduct Commission (**LECC**), modelled on the protections in the PID Act. This was in part due to a report in November 2017 from the Joint Parliamentary Committee on the Independent Commission Against Corruption (**ICAC Committee**), entitled *Protections for People who make Voluntary Disclosures to the ICAC*.[55]

The ICAC Committee found that the protections for people who made disclosures to the ICAC were too narrow and unclear in their application. The ICAC Committee found that there was significant public interest in increasing the protections available to people who make voluntary disclosures to the ICAC. It appeared to the ICAC Committee that the current lack of protection was deterring people from making voluntary disclosures to the ICAC, and thereby stopping the detection, exposure and prevention of corrupt conduct. The ICAC Committee accordingly recommended amendments to the *Independent Commission Against Corruption Act 1988* (**ICAC Act**) to protect people who make voluntary disclosures to the ICAC against criminal, civil and disciplinary liability for doing so.[56]

5.2.4.1 Laws that protect people who choose to whistle-blow from criminal liability

The table at Appendix B sets out some of the laws that protect members of the public from criminal liability for making voluntary disclosures of misconduct or wrongdoing to certain bodies. The specific requirements for a disclosure to attract protection under each Act are included in the table, but in summary the protections can apply to disclosures:

- to **ICAC** about corrupt conduct connected to a NSW public official[57]
- to the **National Anti-Corruption Commissioner** or the **Inspector-General of Intelligence and Security** about corrupt conduct connected to a Commonwealth public official[58]
- to the **LECC** about serious wrongdoing by the NSWPF or NSW Crime Commission[59]
- to the **NSW Ombudsman** about serious maladministration by a public authority[60]
- to the **Children's Guardian** about the response of a relevant agency to a report of harm to a child[61]
- to the **Secretary of DCJ** about a child or young person at risk of significant harm[62]
- to the **NSW Ageing & Disability Commissioner** about an adult with disability or older adult who is subject to, or at risk of abuse, neglect of exploitation[63]
- to the **National Disability Insurance Agency** or the **NDIS Quality and Safeguards Commissioner** about an NDIS provider who has, or may have, contravened a provision of the *National Disability Insurance Scheme Act 2013* (Cth).[64]

---

[55] New South Wales, *Parliamentary Debates*, Legislative Assembly, 29 March 2022, 8934-5 (Mark Speakman, Attorney General).

[56] Committee on the Independent Commission Against Corruption, Parliament of New South Wales, *Protections for People who make Voluntary Disclosures to the Independent Commission Against Corruption* (Report, November 2017), iv.

[57] *Independent Commission Against Corruption Act 1988 (NSW).*

[58] *National Anti-Corruption Commission Act 2022* (Cth).

[59] *Law Enforcement Conduct Commission Act 2016* (NSW).

[60] *Ombudsman Act 1974* (NSW).

[61] *Children's Guardian Act 2019* (NSW).

[62] *Children and Young Persons (Care and Protection) Act 1998* (NSW).

[63] *Ageing and Disability Commissioner Act 2019* (NSW).

[64] *National Disability Insurance Scheme 2013* (Cth).

The laws in relation to each of the above authorities contain a provision substantially similar to s 40 of the PID Act and s 10 of the Cth PID Act, which protects against criminal liability, as well as civil and administrative/disciplinary liability, for the act of voluntarily disclosing information to the relevant authority (referred to for the remainder of this report as '**whistleblower protection provisions**').

Example of a whistleblower protection provision:

National Anti-Corruption Commission Act 2022 (Cth)

Section 24 Protection of persons from liability:

(1) If a person makes a NACC disclosure:

(a) the person is not subject to any civil, criminal or administrative liability (including disciplinary action) for the NACC disclosure; and

(b) no contractual or other remedy may be enforced, and no contractual or other right may be exercised, against the person on the basis of the NACC disclosure.

Each of the whistleblower protection provisions listed in the third column of the table at Appendix B would operate to protect the people who make the disclosures from liability under ss 11 and s 14 of the SD Act for those disclosures if the disclosures included illegal surveillance material. Each of the Acts which contain a whistleblower protection provision makes clear that the protection for liability is **only for the act of disclosing the information to the authority** – the protection does not extend to any past illegal conduct that the discloser may have engaged in to obtain the information.

However, the ICAC Act, the *Law Enforcement Conduct Commission Act 2016* (**LECC Act**) and the *Ombudsman Act 1974* also contain a provision similar to s 41 of the PID Act, pursuant to which the Attorney General may give an undertaking that a disclosure of past illegal conduct which occurs as part of whistleblowing will not be used in evidence in criminal or civil proceedings against the discloser.

So for example, if Person A:

- makes a disclosure to an authority listed in Appendix B which meets the requirements for protection under the relevant Act, and
- the information in the disclosure includes a video recording made by using an optical surveillance device in breach of s 8 of the SD Act, and
- in making the disclosure Person A discloses that they used an optical surveillance device in breach of the SD Act

then:

- under the criminal liability protection provisions, Person A will be **protected from liability under s 11 of the SD Act** for communicating the video recording as part of the making the disclosure. It is unclear if the person would still be liable for possessing the video recording under s 12 of the SD Act.
- under the ICAC Act, LECC Act and *Ombudsman Act 1974* the Attorney General would have the discretion to give Person A an undertaking that their admission that they breached s 8 of the SD Act will not be used as evidence against them in any criminal prosecution under s 8 of the SD Act.

5.2.4.2 Laws that protect people from criminal liability when required to provide information or records

The analysis in 5.2.4.1 above focused on laws that provide protections from criminal liability for when people **voluntarily** provide information to an agency. There are other laws (and other provisions in

the laws discussed above) which contain protections for people who are **required** by an agency to provide information, documents or records relevant to an investigation or assessment of a complaint.

For example, under s 9 of the *Ombudsman Act 1974* (Cth), where the Commonwealth Ombudsman has reason to believe that a person is capable of furnishing information or producing documents or other records relevant to an investigation under that Act, the Ombudsman can issue a notice to the person requiring them to provide that information/document/record.

It is an offence for the person not to provide the requested material,[65] and a person is not excused from providing it on the ground that to do so would contravene the provisions of any other statute, or might tend to incriminate the person or make the person liable to a penalty.[66] However s 9 of the *Ombudsman Act 1974* (Cth) provides that:

- a person is not liable to any penalty under the provisions of any other statute by reason of his or her furnishing information, producing a document or other record or answering a question when required to do so under this Act (s 9(5)) and
- the information, the production of the document or record is not admissible in evidence against the person in proceedings (other than offences against the Ombudsman Act 1974 (Cth) or for giving false or misleading information) (s 9(4)(c) and (d)).

This means that if a person is required under s 9 to provide a record or information which was created/obtained from illegally using a surveillance device contrary to the SD Act, s 11, 12 or s 14 of the SD Act will not provide an excuse for the person not to provide the information or record, but the person will not be liable under those sections for doing so.

5.2.5 Sections 316 and 316A of the Crimes Act

In discussing laws relating to whistleblowers, it is relevant to consider s 316 of the Crimes Act. That section makes it an offence to conceal a serious indictable offence. An offence against s 316 is punishable by to 5 years' imprisonment (depending on the maximum penalty for the offence that was concealed).

S 316 applies where an adult:

- knows or believes that a **serious indictable offence**[67] **has been committed** by another person, and
- knows or believes that he or she has **information that might be of material assistance** in securing the apprehension of the offender or the prosecution or conviction of the offender for that offence, and
- **fails without reasonable excuse** to bring that information to the attention of a member of the NSW Police Force or other appropriate authority.

The Crimes Act does not define what will constitute a reasonable excuse for the purpose of avoiding liability under s 316, except for providing that it will be a reasonable excuse if the information relates to a sexual offence or a domestic violence offence against an adult person (the alleged victim), and the person believes on reasonable grounds that the alleged victim does not wish the information to be reported to police or another appropriate authority.[68]

Section 316A of the Crimes Act provides a similar offence for failing to bring information about a child abuse offence to the attention of police without reasonable excuse. Section 316A(2) includes a

---

[65] *Ombudsman Act 1976* (Cth) s 36(1)(ba) and (c).

[66] *Ombudsman Act 1976* (Cth) s 9(4).

[67] A serious indicatable offence is an indictable offence that is punishable by 5 or more years' imprisonment: *Crimes Act 1900*, s 4.

[68] *Crimes Act 1900* (NSW) s 316(1A).

non-exhaustive list of circumstances which will constitute a reasonable excuse. The list does not mention if the disclosure to police will contravene another law.

The Crimes Act therefore does not indicate whether the fact that disclosure will contravene a law is a reasonable excuse under s 316 or s 316A.

The majority of the High Court in *Taikato v the Queen* stated that although 'the term "reasonable excuse" has been used in many statutes and is the subject of many reported decisions':

> decisions on other statutes provide no guidance because what is a reasonable excuse depends not only on the circumstances of the individual case but also on the purpose of the provision to which the defence of "reasonable excuse" is an exception.[69]

The majority of the High Court also stated that:

> the reality is that when legislatures enact defences such as "reasonable excuse" they effectively give, and intend to give, to the courts the power to determine the content of such defences. Defences in this form are categories of indeterminate reference that have no content until a court makes its decision. They effectively require the courts to prescribe the relevant rule of conduct after the fact of its occurrence. That being so, the courts must give effect to the will of Parliament and give effect to their own ideas of what is a "reasonable excuse"...[70]

In terms of the purpose of s 316 (and now also s 316A), in *Wilson v Director of Public Prosecutions (NSW)* Meagher JA (with whom Bathurst CJ and Basten JA agreed) explained that:

> By punishing the withholding of information, believed to be material in securing a conviction, by someone who knows or believes such an offence has been committed, the provision operates as a deterrent to people who might otherwise withhold information from the police. In doing so it furthers the more general objective that members of the public report information and beliefs about serious offences to the police so as to assist in the apprehension, prosecution and conviction of offenders.[71]

5.2.5.1 Relationship between ss 11 and 14 of the SD Act and s 316 of the Crimes Act

When considering the relationship between the offences in ss 11, 12 and 14 of the SD Act and ss 316 and 316A of the Crimes Act, it is relevant to consider the analysis of s 316 by Schmidt AJ in *Wood v Secretary of the Department of Transport*.[72] In that case Transport NSW had summarily dismissed one of its employees, Mr Wood, because he had provided information held by Transport NSW to police to assist them in a murder investigation.

The case concerned the question whether Transport NSW was entitled to dismiss Mr Wood. In the course of submissions Transport NSW argued that either the confidentiality provisions in Mr Wood's employment contract or the offence in s 62 the NSW Privacy Act precluded Mr Wood from disclosing the information to police and therefore constituted a 'reasonable excuse' for the purpose of s 316 of the Crimes Act.

Acting Justice Schmidt found that **s 316 of the Crimes Act in effect imposes a legal obligation on every person to disclose information about criminal offences to relevant authorities**. Her Honour explained that 'At common law the existence of an obligation to provide information about criminal offences to authorities has long been recognised'.[73] Her Honour stated that when the common law offence of misprision of felony was abolished with the enactment of s 316 of the Crimes Act, '[t]hat did not abolish the obligation to assist police, but rather reformed the circumstances in which an offence will be committed, when information is not disclosed.'[74]

---

[69] *Taikato v The Queen* (1996) 186 CLR 454, 464.

[70] *Taikato v The Queen* (1996) 186 CLR 454, 466.

[71] *Wilson v Director of Public Prosecutions (NSW)* [2017] NSWCA 128, [45].

[72] [2021] NSWSC 1248.

[73] Ibid at [167]. Her Honour cited *A v Hayden (No 2) (*1984) 156 CLR 532 at 555.

[74] [2021] NSWSC 1248 [168].

Her Honour concluded that Mr Wood had a legal obligation under s 316 to provide the information to police. In relation to the effect of the contractual confidentiality provision, Schmidt AJ stated the principle that '[t]**he public interest in disclosure of iniquity, that is serious crime, will always outweigh the public interest in the "preservation of private and confidential information**".[75] Her Honour continued:

> A person who commits a criminal offence can have no right to privacy or confidentiality in such information, notwithstanding the provisions of an employment contract, privacy policies or the provisions of the Privacy and Personal Information Protection Act, to which I will return.
>
> An employer and employee cannot contract out of provisions such as ss 315, 315A and 316 of the Crimes Act. Nor can a contractual confidentiality obligation lawfully prevent the provision of information about offending which it might capture, to police. If it purports to do so, the contract will be contrary to public policy and either read down, or not enforced.[76]

Her Honour then turned to Transport NSW's argument in relation to s 62 of the NSW Privacy Act. That section, titled 'corrupt disclosure and use of personal information by police sector officials', makes it an offence for a public sector official, otherwise than in correction with the lawful exercise of their functions, to intentionally disclose or use any personal information about another person to which the official has or had access in the exercise of his or her official functions.

Transport NSW argued that after the enactment of s 62, disclosure by a public official to whom s 62 applies would no longer be required under s 316. That was because the s 62 offence would provide a reasonable excuse for the official not disclosing to police personal information which he or she knew or believed might be of material assistance in securing the apprehension, prosecution or conviction of an offender for a serious indictable offence: s 316(1)(C).

Acting Justice Schmidt rejected this argument, stating:

> I am not persuaded that this was contemplated by the enactment of s 62. That would have been a very important alteration to the law, with significant adverse ramifications for the apprehension, prosecution and conviction of offenders for serious indictable offences. I am satisfied that this is not what the Legislature intended. Certainly nothing of that kind is hinted at in the Second Reading Speech…To the contrary, there it was observed that "It should be stressed that the data protection principles are generally subject to any specific provision in any law relating to the use or disclosure of information": … Section 316 of the Crimes Act is such a law and an important one.[77]

There is similarly nothing in the Second Reading Speech to the SD Act to suggest that when enacting ss 11 and 14 of the SD Act, Parliament contemplated that those offences would provide a 'reasonable excuse' preventing the operation of the obligation in s 316. The thrust of the speech on the SD Act was its role in supporting law enforcement agencies to investigate and prosecute serious crimes such as murder, terrorism, and drug manufacture and importation, through providing them with the authority to lawfully use surveillance devices under the warrant scheme in the Act. It would therefore seem somewhat incongruent if s 11 and s 14 in that SD Act would operate to prevent disclosure of information about serious indictable offences to police, by undermining the obligation in s 316.

---

[75] [200] (citing *A v Hayden (No 2)* (1984) 156 CLR 532 at 545.

[76] [208]-[209].

[77] [235]-[236].

6 DCJ's analysis and recommendations

Summary of DCJ's recommendations

Below is a list of DCJ's recommendations for amendments to the SD Act that are discussed in this chapter. The flowchart on page 7 illustrates the interaction between the different proposed amendments (other than Recommendations 5 and 6).

Recommendation 1 - ***Amendment to offence for possession of material in s 12***

Section 12 of the SD Act should be amended so that it is only an offence for a person to possess a record of a private conversation or an activity when:

(a) the person was involved in the record being obtained, directly or indirectly, by use of a listening device, optical surveillance device or tracking device in breach of Part 2 of the SD Act

(b) the person caused a third party to obtain the material by using a device illegally, or

(c) the person knows that the record was obtained through the illegal use of a surveillance device and fails to give the record to an investigative body within a reasonable period of time after becoming aware that the record was obtained illegally

Paragraph (c) should not apply to an officer of an investigative body in possession of a record in connection with the exercise of the investigative body's investigative functions.

Recommendation 2 - ***Exceptions to s 11 and s 14 for communication and publication to investigative bodies***

The SD Act should be amended:

(a) To include in s 11 and s 14 of the SD Act an exception that the offences in those sections will not apply to communication or publication to an investigative body that is in the public interest and to clarify that communication or publication to an investigative body for the purposes of exercising its investigative functions is in the public interest

(b) To include a definition of 'investigative body' that includes any department, agency, authority or organisation that has statutory powers under a NSW or Commonwealth law to investigate any matters.

Recommendation 3 – ***Exceptions to s 11 and s 14 for communication and publication by investigative bodies and prosecuting authorities***

Section 11 and section 14 of the SD Act should be amended to include an exception that the offences in those sections will not apply to communication or publication of illegal surveillance material:

- by any person working in an investigative body or a prosecuting authority
- in accordance with their statutory functions and obligations
- to any person (including another investigative body or a prosecuting authority)
- unless the person who communicates or publishes the material knows that a current or former employee of the investigative body or prosecuting authority was involved in the surveillance device being used in breach of the SD Act to obtain the material, including causing another person to use the device illegally.

Recommendation 4 – *Exceptions to s 11 and 14 for re-publication*

Section 11 and 14 of the SD Act be amended to insert exceptions which provide that it is not an offence under those sections for a person (the re-publisher) to communicate or republish illegal surveillance device material that another person or body has already been published to the world at large, unless the re-publisher knows the original publication of the material was in breach of s 11 or 14 of the SD Act.

Recommendation 5 – *Requirement for a statutory review 5 years after commencement*

The SD Act be amended to include a requirement that the Minister commence a statutory review of the amendments proposed in this report as soon as practicable after 5 years after the commencement of the amendments.

6.1 Amending the possession offence in s 12 of the SD Act

Section 12 of the SD Act makes it a criminal offence for a person to possess a record of a private conversation or an activity if the person knows that the record has been obtained, directly or indirectly by use of a listening device, optical surveillance device or tracking device in breach of sections 7, 8 or 9 of the SD Act. This offence applies to a person even if they were not in any way involved in the illegal use of the device.

A majority of submissions supported a public interest exception of some type being inserted into s 12. Some of the reasons provided by stakeholders included:

- There are occasions when a person, including a child or young person, may inadvertently come into possession of information in contravention of section 12 of the SD Act, for example they may be sent a recording via messages or social media.
- Records may be sent to persons or investigative agencies anonymously, making it difficult for the person or agency to determine whether the recording was made in breach of the SD Act.
- The offence effectively prevents law enforcement and investigative agencies that receive unsolicited records from viewing or using such records, even if they may be relevant to an investigation.
- The surveillance devices laws in Victoria, South Australia and the Northern Territory do not criminalise possession of a record from a surveillance device, and the law in Western Australia which does contain a possession offence has an exception for possessing records obtained as a result of use of a device in the public interest.

One stakeholder submission recommended that s 12 should be removed in its entirety, to align with the law in Victoria, South Australia and the Northern Territory and avoid criminalising possession of records that were unsolicited.

Other stakeholders submitted that the exception to s 12 should be crafted to only apply to persons who were not complicit in the creation of the record in breach of the SD Act. These stakeholders were concerned that if a public interest exception to s 12 extended to persons who had been involved in the breach of ss 7, 8 or 9 of the SD Act, this would in effect encourage such breaches.

Two stakeholder submissions highlighted the practical difficulty that would be faced by agencies if an exception to s 12 was conditional on the possession of the record being 'reasonably necessary in the public interest'. Those submissions noted that in order for an agency to determine whether possession of a record is reasonably necessary in the public interest, the agency would need to review (and therefore possess) that material, and therefore risk being in breach of SD Act if they subsequently determine that possession of the record did not meet that threshold. Inclusion of such a threshold requirement may therefore undermine the effectiveness of the exception.

6.1.1 DCJ's conclusions

DCJ accepts the point regarding the practical difficulties that would arise if an exception to s 12 included the requirement that possession be 'reasonably necessary in the public interest'. This problem would arise even if the exception permitted possession simply 'in the public interest'. Any qualification of the exception would require the person or agency who is given a record to review the contents of the record, and therefore risk breaching the SD Act before they can form a view as to whether their possession fell within the exception.

DCJ notes that in fact the current knowledge requirement in s 12 creates the same practical difficulties. A person or agency that has received an unsolicited surveillance device record will not be able to form a view as to whether or not it has been obtained by use of a device in breach of the SD Act without reviewing the contents of the record. This may in effect prevent an officer or agency from reviewing a record which may be relevant to an investigation. DCJ notes that part of the reason that ICAC was granted an exemption to parts of the SD Act was due to the public interest in ICAC being able to possess records of private conversations which had been made by a third party, in order to use such records in its investigations.

For these reasons, instead of an exception, DCJ proposes that the record possession offence in s 12 be amended so that the offence only applies to persons who were complicit in the use of a surveillance device contrary to ss 7, 8 or 9 of the SD Act which resulted, directly or indirectly, in the record being obtained. This should include persons who in any way caused a third party to use the device in breach of ss 7, 8 or 9. The offence should also apply to people who are aware of the provenance of the record and who are not or have not turned the material over to investigative agencies.

This proposed amendment would:

- appropriately focus the criminal sanctions in s 12 on persons who were in some way responsible for use of a surveillance device in breach of the SD Act or who were aware of the provenance of the material and did not/did not intend to pass the record on to an investigative agency, and
- ensure that persons and agencies who in good faith happen to come into possession of illegal surveillance device records without being involved in the illegality which led to their creation do not face criminal liability.

DCJ's proposed amendment would also align s 12 with the comments from the majority of the High Court in *Farm Transparency*. As discussed above in Part 3.1, in that case the majority decision of the Court clearly suggested that the burden that s 12 of the SD Act places on the implied constitutional freedom of political communication may not be justified in circumstances where the person who possessed the record was not complicit or involved in the breach of the SD Act through which the record was obtained.

In relation to the absence of a record possession offence in Victoria, South Australia and the NT, DCJ notes that those jurisdictions criminalise communication or publications of records obtained as a result of both **legal and illegal** use of surveillance devices. As NSW only criminalises communication and publication of illegally-obtained records, retaining a possession offence targeting illegally-obtained records aligns with the different approach taken in the NSW SD Act.

Recommendation 1

Section 12 of the SD Act should be amended so that it is only an offence for a person to possess a record of a private conversation or an activity when:

(a) the person was involved in the record being obtained, directly or indirectly, by use of a listening device, optical surveillance device or tracking device in breach of Part 2 of the SD Act
(b) the person caused a third party to obtain the material by using a device illegally, or
(c) the person knows that the record was obtained through the illegal use of a surveillance device and fails to give the record to an investigative body within a reasonable period of time after becoming aware that the record was obtained illegally

Paragraph (c) should not apply to an officer of an investigative body in possession of a record in connection with the exercise of the investigative body's investigative functions.

6.2 Exceptions to ss 11 and s 14 for communication and publication to and by investigative bodies

6.2.1 The need for new exceptions

DCJ agrees with the significant majority of stakeholders that s 11 and s 14 of the SD Act should be amended to allow for a private conversation or a record of an activity, or a report of a private conversation or an activity obtained as a result of a contravention of ss 7, 8, 9 of 10 of the SD Act (referred to for the remainder of this report as '**illegal surveillance material**') to be communicated and published in certain circumstances when such communication and publication would serve the public interest.

DCJ acknowledges that ss 11 and 14 promote the public interest in protecting persons' privacy by criminalising communication and publication of material obtained through illegal surveillance. However, this needs to be weighed against the competing public interest in persons providing evidence of crimes to police, and evidence of other wrongdoing or risks to vulnerable persons to bodies with statutory powers and responsibilities to investigate, and those investigative bodies being able to execute their functions to investigate, address and expose crimes and wrongdoing, and address risks to vulnerable persons.

DCJ considers that there are compelling reasons to conclude that the offences in s 11 and s 14 of the SD Act do not appropriately balance these competing public interests.

The provisions as currently drafted make it a criminal offence, punishable by up to five years' imprisonment, for a person to provide illegal surveillance material to police or other relevant authorities. There is no exception for material that it is evidence of a crime or other illegal conduct. This undermines the obligations in s 316 and s 316A of the Crimes Act to provide information about serious indictable offences and child abuse offences to police or relevant authorities.

Also, as noted in Part 5.2 above, a number of NSW and Commonwealth laws already in effect permit persons to provide illegal surveillance material to certain statutory agencies, despite ss 11 and 14 of the SD Act, if the material meets the requirements to attract protection under the whistleblower protection provisions in those Acts. In some cases, section 316 of the Crimes Act would require it. Sections 11 and 14 of the SD Act should reflect those protections.

DCJ acknowledges the concerns raised by some stakeholders that public interest exceptions to s 11 and 14 will encourage persons, including law enforcement officers, to use surveillance devices in breach of ss 7, 8, 9 and 10 of the SD Act by allowing them to communicate or publish the material obtained. Some stakeholders submitted that such exceptions will therefore lead to trespasses and breaches of privacy.

DCJ notes that any persons, including law enforcement officers, who knowingly use surveillance devices in breach of ss 7, 8, 9 or 10 of the SD Act will face criminal liability under those sections (and potentially under s 12). A breach of any of those sections can attract a sentence of up to 5 years' imprisonment.

As set out in Part 5.1 above, conduct that breaches ss 7, 8, 9 or 10 of the SD Act may also breach other laws which protect private property and privacy and attract further legal consequences. For example, if a person trespasses on another person's property and uses an optical surveillance device in breach of s 8 of the SD Act, the person will be criminal liable under the ILP Act if the property is inclosed lands, and may be sued for the tort of trespass or nuisance. DCJ considers that, even if public interest exceptions are included in ss 11 and 14 of the SD Act, there are sufficient deterrents in criminal and civil laws against use of surveillance devices contrary to the SD Act.

DCJ also notes that the NSW and Cth laws which protect privacy both recognise that there are countervailing public interests which may override the public interest in protecting privacy in certain circumstances. The NSW Privacy Act contains considerable exemptions for law enforcement agencies and investigative agencies. The new tort for serious invasions of privacy in the Cth Privacy Act includes a list of 'countervailing public interests' which the court may consider outweighed the public interest in protecting the plaintiff's privacy.

DCJ accordingly concludes that it is appropriate to amend ss 11 and 14 of the SD Act to ensure that those sections allow for the public interest in persons providing relevant information to investigating authorities, and in those authorities being able to use that information in the exercise of their statutory functions.

The specific aspects of DCJ's proposed exceptions in relation to the functions of investigative bodies are discussed under the subheadings below.

6.2.2 Exceptions should not be limited to material showing unlawful or corrupt conduct

6.2.2.1 Criminal or unlawful conduct

Section 11 of the SD Act prohibits a person from publishing, or communicating to any person, a private conversation or a record of an activity, or a report of a private conversation or an activity, that has come to the person's knowledge as a direct or indirect result of the use of a listening device, optical surveillance device or a tracking device in contravention of ss 7, 8 or 9 of the SD Act.

Section 14 of the SD Act makes it an offence of a person to publish or communicate to any person any information regarding the input of information into, or the output of information from a computer if the information was obtained as a direct or indirect result of the use of a data surveillance device contrary to s 10.

The current effect of s 11 and s 14 is that it will generally be a criminal offence if:

- A person provides the illegal surveillance material to police or other relevant authorities because it is evidence of a crime or other illegal conduct (and even if the person was not involved in illegally obtaining the material).
- An agency that has statutory responsibilities to investigate offences, corrupt conduct or other misconduct or wrongdoing, uses or publishes the illegal surveillance device material they receive from other parties because it is relevant to their investigation.

There are only limited exceptions to the above, for example if all the parties to the recorded private conversation or activity consent,[78] or if the communication or publication by the person or the

[78] *Surveillance Devices Act 2007,* s 11(2)(a)(ii).

agency is no more than in reasonably necessary in connection with an **imminent threat** of serious violence to persons, substantial damage to property or commission of a serious narcotics offence.[79]

There was a high level of support from stakeholders for a public interest exception to ss 11 and 14 to permit the communication or publication or illegal surveillance material that may constitute evidence of a crime or unlawful conduct.

DCJ notes that the offences in s 11 and s 14 appears to conflict with the common law duty to provide information about criminal offences to authorities, discussed by Schmidt AJ in *Wood v Secretary of the Department of Transport*, discussed in 5.2.5.1 above. Sections 11 and 14 also appear to undermine the statutory obligations, with criminal penalties, that the offences in s 316 and 316A of the Crimes Act seek to impose on all persons to provide information about serious indictable offences and child abuse offences to police and relevant authorities.

6.2.2.2 Other wrongdoing and risks to vulnerable persons

A number of stakeholder submissions stated that the public interest exceptions should not be limited to communication or publication of content about unlawful conduct, as there can be public interest in other types of content being communicated or published. Stakeholders pointed out, for example, that:

- ICAC has jurisdiction over corrupt conduct, which may not be unlawful conduct, and has been granted an exemption for its work in the SD Regulation.
- The LECC has jurisdiction over misconduct and maladministration by police officers and NSW Crime Commission officers
- If the NSW Trustee and Guardian receives information relating to allegations of violence, abuse or neglect or exploitation of one of its customers, it has a responsibility to act on that information.
- the offences in the SD Act may hinder DCJ and the Office of the Children's Guardian using illegal surveillance material that raises a reasonable belief that a child is at significant risk of harm under *Children and Young Persons (Care and Protection) Act 1998* in their child protection functions under that Act
- there have been examples of the parents of adult children with disability who are living in supported accommodation installing cameras in the accommodation to record suspected abuse of their child by carers.[80]
- severe neglect, abuse or exploitation of a participant's vulnerability may not meet the threshold of a criminal offence but is still unconscionable conduct that warrants investigation by the NDIS Quality and Safeguards Commission and accountability in the public interest.

As discussed in Part 5.2 above, the whistleblower protection provisions in a number of NSW and Commonwealth laws protect persons from criminal liability for disclosing information to certain authorities (including ICAC, the LECC, the Children's Guardian, the Secretary of DCJ and the NDIS Quality and Safeguards Commissioner) about a range of different types of wrongdoing or risks to vulnerable persons, not just criminal conduct. It appears these provisions in effect protect persons against liability under s 11 and s 14 if the information disclosed included, or was derived from, illegal surveillance material. Such provisions demonstrate that there are a variety of circumstances in

[79] *Surveillance Devices Act 2007*, s 11(2)(b).

[80] A stakeholder submission referred to the Victorian case of Ms Lee-Anne Mackey, whose abuse by her carers was captured on an optical surveillance device installed in Ms Mackey's bedroom by her father. As a result three of Ms Mackey's carers were sentenced for assaults against Ms Mackey. Ms Mackey's case, including the relevance of the surveillance device footage, is discussed in *Moutsos v Kinghorn* [2023] VCC 459.

which the public interest in certain information being disclosed to authorities requires other criminal law prohibitions to be overridden.

Some stakeholder submissions pointed out that it can be in the public interest for persons to expose the gaps in existing laws so that such gaps can be addressed. One such stakeholder submitted that 'a morally questionable or harmful practice that is permitted by law may need to be exposed and brought to public attention to show the law is failing to achieve its intended purpose or misaligned with community expectations'.

One stakeholder also submitted that DCJ consider circumstances where possession, communication or publication of illegal surveillance material may be necessary to prevent or lessen a serious and imminent threat to the life or health of any person, for example in respect of infectious disease control.[81]

6.2.2.3 DCJ conclusion

DCJ agrees that the public interest exceptions to s 11 and s 14 should not be limited to content about unlawful conduct. At a minimum, the exceptions should cover communication of content about all the types of wrongdoing and risks to vulnerable persons that attract statutory protection as discussed in Part 5.2.

However DCJ does not consider it appropriate to limit the categories of content to those that are subject to those whistleblower protection provisions. DCJ agrees with those stakeholders who submitted that it can be in the public interest for persons to expose gaps in legal frameworks by revealing conduct that is not prohibited or regulated but may need to be. Also, DCJ notes that there do not appear to be any whistleblower protection provisions that protect a member of the public from criminal liability for providing information relating to a serious crime to police. It would be incongruent for a person to be protected from criminal liability under ss 11 and 14, for example for providing illegal surveillance material concerning a matter of serious maladministration to the NSW Ombudsman, but to be criminally liable for providing illegal surveillance material that is evidence of a crime to police.

Two stakeholders submitted that there is a risk that public interest exceptions to s 11 and 14 will result in officers in law enforcement agencies bypassing the warrant scheme in the SD Act by illegally using surveillance devices to obtain material concerning crimes that they then pass on to law enforcement agencies. One of the stakeholders submitted that there should accordingly be limitations on who can communicate material to law enforcement agencies under the exception.

As discussed above in the introduction to this part, DCJ considers there are sufficient other deterrents in the SD Act and under other laws to dissuade law enforcement officers from using surveillance devices in breach of ss 7-10 of the SD Act. These include the criminal penalties under ss 7-10 and s 12 of the SD Act, and under the ILP Act, as well as the possibility of being sued for trespass, nuisance or (soon) a serious invasion of privacy. DCJ does not consider it necessary or appropriate to exclude law enforcement officers from being able to rely on the exception to ss 11 and 14 of the SDF Act. DCJ notes that a law enforcement officer may become aware of illegal surveillance material obtained by another person using a surveillance device illegally and considers that material should be communicated to an investigative body in the public interest.

6.2.3 Exceptions should cover material from all types of surveillance devices

A few stakeholders raised questions about whether material from illegal use of a data surveillance device should be able to be communicated or published in the public interest.

---

[81] The stakeholder referred to the exception in s 18(c) of the *Privacy and Personal Information Protection Act 1998*.

A data surveillance device is defined in s 4 of the SD Act as **any device or program** capable of being used to record or monitor the input or output of information into or from a computer, but does not include an optical surveillance device. A computer is defined as 'any electronic device for storing, processing or transferring information', and therefore would include a mobile phone with internet access.

Section 10 of the SD Act prohibits use of a data surveillance device on a computer if the use involves entry onto premises without consent, or interference with a computer on premises without consent of the person in lawful possession or control of the computer.

While a majority of stakeholder submissions generally expressed support for public interest exceptions for ss 11, 12 and 14 of the SD Act collectively, only a small number of submissions specifically commented on a public interest exception for s 14. One stakeholder noted the 'potential security considerations involved in relation to data surveillance devices' but supported an exception to s 14 that would allow communication or publication of illegal surveillance material from a data surveillance device to police, other law enforcement agencies, and anti-corruption and integrity bodies about serious criminal matters or unlawful corrupt activity that is 'no more than reasonably necessary in the public interest'.

One stakeholder noted that the public interest exceptions for publication and communication in the surveillance devices laws in other Australian jurisdictions did not extend to information from a data surveillance device. DCJ notes that while this is true, part of the reason for this position may be that the surveillance devices laws in the Northern Territory and in Victoria only make it an offence for **law enforcement officers** to use a data surveillance device,[82] and the law in Western Australia does not include any offence for use of data surveillance devices.[83] It appears in these jurisdictions it was not anticipated (or was not of concern) that members of the public may have access to and use data surveillance devices.

Only the *Surveillance Devices Act 2016* (SA) contains an offence for use of a data surveillance device by any person.[84] That Act does not include any public interest exception for communication or publication of information obtained by using such a device.

One stakeholder indicated that data obtained from an illegal use of a data surveillance device may provide evidence of coercion or abuse in the context of domestic violence which should be able to be passed on to police.

DCJ considers that there are scenarios in which a person may come into possession of information from an illegal use of a data surveillance device which it is in the public interest for that person to provide to an investigative body. For example, it has been reported that perpetrators of domestic and family violence often use technology to track or monitor their targets.[85] This includes 'spyware' or 'stalkerware' which is an application or software that when installed on a person's computer or mobile phone can send the user information about the data going in and out of the computer or phone.[86]

A victim or third party (for example a support worker) may become aware of information that a domestic violence perpetrator has obtained from the victim's computer or mobile phone using software that meets the definition of a data surveillance device. The victim or third party should not

---

[82] *Surveillance Devices Act 2007* (NT), s 16; *Surveillance Devices Act 1999* (Vic) s 12.

[83] Surveillance Devices Act 1998 (WA).

[84] *Surveillance Devices Act 2016* (SA) s 8.

[85] See for example ESafety Commissioner, 'Domestic Violence', https://www.esafety.gov.au/key-topics/domestic-family-violence; ANROWS, 'Technology-facilitated abuse: Extent, nature and responses in the Australian Community', https://www.anrows.org.au/project/technology-facilitated-abuse-extent-nature-and-responses-in-the-australian-community/; NSW Police Force, 'Technology Facilitated Abuse', https://www.police.nsw.gov.au/crime/domestic_and_family_violence/technology_facilitated_abuse.

[86] See for example Patrick Begley, *Toxic Mix of spyware and jealous spouses*, Sydney Morning Herald, 18 March 2024 (attachment to SGM24/2739).

be criminalised for providing that information to police or another investigative body, and an investigative body should not be prohibited from using that information in an investigation.

DCJ also considers that it is possible that information from a data surveillance device may also provide evidence of crimes in other contexts, for example corrupt conduct.

DCJ proposes that s 14 of the SD Act should permit a person to provide material obtained from illegal use of a data surveillance device to investigative bodies, and permit those bodies to use that material, under public interest exceptions, in the same way as material from other surveillance devices.

6.2.4 Communication and publication to investigative bodies

A significant number of stakeholder submissions supported exceptions that permit persons to communicate and publish illegal surveillance device material to police, other law enforcement agencies, regulatory enforcement agencies, anti-corruption and integrity bodies.

DCJ notes that in 2007 when the SD Act was passed by Parliament law enforcement agencies were the primary users of surveillance devices. The use of surveillance devices in the community has increased exponentially since 2007, alongside developments in technology. In 2025 it has become normalised for members of the public to have a surveillance device on their person at all times in the form a mobile phone that can record audio and video and take photographs and send them to contacts or share them online.

Given the widespread and everyday community use of surveillance devices, the likelihood of members of the public coming into possession of illegal surveillance material that it may be in the public interest for the person to pass on to relevant authorities has increased.

As noted in Part 5.2 above, a number of NSW and Commonwealth laws already in effect permit persons to provide illegal surveillance material to certain statutory agencies, despite s 11 and s 14 of the SD Act, if the material meets the requirements to attract protection under the whistleblower protection provisions in those Acts. When the NSW Parliament or Commonwealth Parliament created the whistleblower protection provisions in those other Acts, it determined that the public interest in information about certain wrongdoing or risks to vulnerable persons being provided to relevant authorities who can investigate such matters overrides the public interest in the person providing the information facing liability under any other criminal prohibition.

DCJ considers that exceptions to ss 11 and 14 of the SD Act should reflect the public interests that are prioritised in the whistleblower protection provisions in other laws, and in ss 316 and 316A of the Crimes Act.

DCJ considers that public interest exceptions to s 11 and s 14 should allow for persons to provide illegal surveillance material to any '**investigative body'**. This term should be broadly defined to include any department, agency, authority or organisation that has been given statutory powers under a NSW or Commonwealth law to investigate certain matters, including all law enforcement agencies. This draws from the definition of 'investigative agencies' for the purposes of exemptions in the NSW Privacy Act, which extends to any (NSW) public sector agencies with investigative functions if —

- those functions are exercisable under the authority of an Act or statutory rule (or where that authority is necessarily implied or reasonably contemplated under an Act or statutory rule), and
- the exercise of those functions may result in the agency taking or instituting disciplinary, criminal or other formal action or proceedings against a person or body under investigation'.[87]

The proposed definition should capture all those authorities to whom disclosures can be made which attract protection under whistleblower protection provisions.

[87] *Privacy and Personal Information Protection Act 1998* s 3 (paragraph (b) of definition of investigative agency).

As discussed in Part 5.2.4, a person may voluntarily provide illegal surveillance device material to an investigative body (for example by lodging a complaint or a report) or a person may be required to provide the material to the body, either because they are under a general statutory duty to report certain information, or because the body exercises a statutory power to require the particular person to provide certain information. The exceptions to ss 11 and 14 should protect the person from liability under all of these scenarios.

6.2.4.1 Thresholds for persons providing illegal surveillance material to investigative bodies

A significant number of stakeholders supported public interest exceptions to s 11 and s 14 being drafted to require either that communication or publication be reasonably necessary (or no more than reasonably necessary) in the public interest, or that the person believes on reasonable grounds that communicating or publishing the material is in the public interest. However a number of stakeholders submitted that the SD Act should include a definition or examples to assist with interpretation of what is in the 'public interest'.

As noted above in 5.2.5, it is well established that there is a general public interest in evidence of crimes being passed on to authorities, and there are already laws in place which permit evidence of other types of wrongdoing or risks to vulnerable persons to be passed on to agencies with statutory powers to investigate those matters. The whistleblower protection provisions in those laws highlight that there is a strong public interest in bodies that have been given statutory functions to investigate wrongdoing by the NSW Parliament or the Commonwealth Parliament being able to receive relevant information to execute those functions.

DCJ considers that including a threshold requirement to the effect that a person will only escape criminal liability for providing information to an investigative body if the communication or publication was reasonably necessary in the public interest would likely deter persons from passing on such information to authorities, which would be contrary to the public interest. As submitted by one stakeholder who supported a qualification of 'no more than is reasonably necessary in the public interest', based on case law:

> in practical terms, such a threshold requirement is likely to be a complex question which calls for a difficult evaluative judgment. The word 'reasonably' imports an objective test and 'necessary' in this context does not mean essential or indispensable but reasonably appropriate and adapted to the particular context. Therefore, importing such a threshold requirement as to whether any act is reasonably necessary necessarily requires an assessment of the conduct with reference to the facts and circumstances that existed at the time of the conduct or act.[88]

DCJ is also concerned that a requirement that the person believe on reasonable grounds that the communication or publication is in the public interest would deter persons from passing on relevant material to investigative bodies, for fear of exposing themselves to criminal liability under the SD Act. It is relevant that the ICAC Committee in its report on *Protections for People who make Voluntary Disclosures to the ICAC,* discussed in 5.2.4 above, recommended that the protections for persons who made voluntary disclosures to ICAC should not be conditional on persons meeting threshold requirements such as the person had an 'honest and reasonable belief' that the corruption had occurred. The ICAC Committee found that such thresholds 'would do little to deter vexatious complaints and may deter people from making genuine complaints for fear of attracting liability'.[89]

DCJ accepts that communication or publication of illegal surveillance material should only be lawful if it is in the public interest, to ensure that the law does not otherwise condone the sharing of material created in breach of privacy rights and through trespass. The exception is designed to allow persons who come into possession of illegal surveillance material to pass the material on to an

---

[88] Citations to case law have been omitted.

[89] Committee on the Independent Commission Against Corruption, Parliament of New South Wales, *Protections for People who make Voluntary Disclosures to the Independent Commission Against Corruption* (Report, November 2017) p iv and pp 8-9.

investigative body that has powers and responsibilities to investigate matters to which the material relates. The term 'public interest' will be defined to capture the communication or publication of material to an investigative body for the purposes of exercising its investigative functions. However, DCJ does not consider it appropriate to require the threshold public interest test to be further qualified by a requirement that it be 'reasonably necessary in the public interest', or based on reasonable grounds that the communication or publication is in the public interest.

6.2.4.2 Concerns raised about protecting privacy and autonomy of victim-survivors

One stakeholder submitted that a public interest exception should be created to enable illegal surveillance material that may be evidence of sexual violence to be provided to police or relevant authorities, but submitted that:

> Given the sensitive nature of sexual violence and the rights of victim-survivors to determine to whom and when a matter is disclosed, the exception should specify the need to obtain informed consent from the victim-survivor, or their legal guardian, prior to sharing any data illegally obtained using a surveillance device.

DCJ acknowledges the importance of protecting the privacy of victim-survivors, particularly of sexual and domestic violence. However DCJ does not consider it appropriate to expose a person to criminal liability if they pass illegal surveillance material concerning a sexual or violent act on to police without first getting the consent of the victim-survivor. Such a requirement would, for example, prevent a third party who does not know the victim, or can't identify the victim from the material, from passing on to the police the material which may be highly relevant to the investigation of a serious offence.

Imposing such a requirement would appear to work contrary to the general public interest in persons providing information about serious crimes to police, as reflected in the common law duty and s 316 of the Crimes Act.

Section 316 of the Crimes Act makes it a criminal offence for a person **not** to provide information about a serious indictable offence to police, unless they have a reasonable excuse. Section 316A contains a similar offence specifically for failing to provide information about a child abuse offence to police without reasonable excuse. Under s 316 it is a reasonable excuse, and therefore a defence against prosecution, if the information relates to a sexual offence or a domestic violence offence, the alleged victim is an adult, and the person believes on reasonable grounds that the alleged victim does not wish the information to be reported to police. There is a similar defence under s 316A.

The proposal from the stakeholder to make the exceptions to criminal liability under s 11 and s 14 of the SD Act conditional on obtaining the victim-survivor's consent would go beyond the protections for the privacy and rights of victim-survivors in s 316, and may in fact undermine compliance with the obligation represented in that offence.

DCJ notes that there are other safeguards outside of the SD Act which protect victim-survivors privacy. For example, s 91Q of the Crimes Act makes it an offence for a person to intentionally distribute an intimate image of another person without the consent of the person, and knowing the person did not consent to the distribution of the image, or being reckless as to whether the person consented to the distribution.

Also, if illegal surveillance material concerning a sexual offence or domestic violence offence is provided to the police, prosecutors will exercise their discretion as to whether to prosecute the matter, and will take into account whether the victim wants the matter to be prosecuted and is willing to give evidence. For example, under the Prosecution Guidelines the Office of the Director of Public Prosecution considers whether it is in the public interest to prosecute a matter, and this includes consideration of the victim's attitude to prosecution.[90]

---

[90] Office of the Director of Public Prosecutions NSW, *Prosecution Guidelines*, 29 March 2021, at https://www.odpp.nsw.gov.au/prosecution-guidance/prosecution-guidelines.

Finally, even if the prosecution chooses to prosecute a matter, the court has a discretion under s 138 of the *Evidence Act 1995* to exclude evidence that has been obtained illegally, which would include evidence obtained in breach of the SD Act. The operation of s 138 of the *Evidence Act 1995* is discussed in more detail in 6.3.2.6 below.

For these reasons, DCJ does not propose to include a requirement in the Recommendation 2 exceptions that the person obtain the consent of the victim before providing illegal surveillance material relating to a sexual offence or a domestic violence offence to an investigating body.

6.2.4.3 DCJ recommendation for communication and publication to investigative bodies

For the reasons outlined above, DCJ concludes that exceptions should be included in s 11 and s 14 of the SD Act to provide that the offences in those sections will not apply to a person communicating or publishing illegal surveillance material to an investigative body in the public interest.

Recommendation 2 – The SD Act should be amended:

(a) To include in s 11 and s 14 of the SD Act an exception that the offences in those sections will not apply to communication or publication to an investigative body that is in the public interest and to clarify that communication or publication to an investigative body for the purposes of exercising its investigative functions is in the public interest.

(b) To include a definition of 'investigative body' that includes any department, agency, authority or organisation that has statutory powers under a NSW or Commonwealth law to investigate any matters.

6.2.5 Communication and publication by investigative bodies

As mentioned above, there is a clear public interest in allowing bodies that have been given statutory functions to investigate wrongdoing to consider and use information relevant to the execution of those functions. This public interest may override the public interest in protecting the privacy of the person to whom the information relates. This is demonstrated, for example, by the provisions in the NSW Privacy Act which exempt law enforcement agencies[91] from having to comply with the duties in that Act,[92] and the provisions which exempt investigative agencies if compliance with the duties:

- 'might detrimentally affect, or prevent the proper exercise of, the agency's complaint handling functions or any of its investigative functions' or
- if use of the information is 'is reasonably necessary in order to enable the agency to exercise its complaint handling functions or any of its investigative functions'.[93]

One stakeholder submission noted that there are different ways an investigative body may come into possession of illegal surveillance material:

- a person may **voluntarily** provide illegal surveillance device material to an investigative body (for example by lodging a complaint or a report) and
- a person may be **under a duty** to notify an investigative body about a particular matter, or an investigative body may exercise a statutory power to **require** a person to provide illegal surveillance material

---

[91] *Privacy and Personal Information Protection Act 1998*, s 23(1) and s 27.

[92] See Appendix A for an outline of the relevant duties under the Privacy Act.

[93] *Privacy and Personal Information Protection Act 1998,* s 24(1) and (2).

- an investigative body may **seize** illegal surveillance material under a statutory instrument such as a search warrant.

For example, the stakeholder submission outlined that in the case of ICAC it is possible that ICAC may (potentially unknowingly) obtain illegal surveillance material through:

- a person making a complaint about corrupt conduct to ICAC under s 10 of the ICAC Act
- a person providing information or records to ICAC under a duty under s 11 of the ICAC Act to notify ICAC of possible corrupt conduct
- ICAC officers seizing material under search warrants under s 40 of the ICAC Act
- ICAC requiring a person to attend ICAC's offices and produce a document or thing for the purposes of an investigation under s 22 of the ICAC Act
- An ICAC Commissioner, as part of an investigation, summoning a person to appear at a private hearing or public inquiry to give evidence or produce documents, or requiring a person appearing at such a hearing to produce a document or a thing, under s 35 of the ICAC Act.

The stakeholder submission pointed out that, but for the exemption for ICAC currently in s 6A of the SD Regulation, ss 11, 12 and 14 of the SD Act would prevent ICAC from reviewing or using any illegal surveillance material it received through the above, even though the material may be highly pertinent to a corruption investigation.

DCJ notes that the current and a former NSW Parliament have acted on two occasions to mitigate the effect of the offences in ss 11, 12 and 14 of the SD Act on ICAC.

In 2009 the NSW Parliament amended the ICAC Act to enable ICAC to lawfully possess, communicate and publish audio recordings of private conversations involving Mr Michael Loch McGurk, who was then deceased. Following the murder of Mr McGurk on 3 September 2009, there were media reports about audio recordings he had made, which gave rise to speculation concerning corruption in the public administration of NSW.

ICAC approached the NSW Government for legislative amendments to allow ICAC officers to lawfully possess and make use of the recording made by Mr McGurk in the exercise of its functions, as it appeared that the recordings may have been made by Mr McGurk in breach of s 7 of the SD Act. On 30 November 2009, Part 9 of Schedule 4 was inserted into the ICAC Act to provide in effect a temporary exemption for ICAC from Part 2 of the SD Act in relation to possession, communication and publication, before 31 December 2010, of recordings of any private conversations to which Mr McGurk was a party.[94]

More recently, as mentioned in 3.2 of this report, in August 2023 s 6A was inserted into the SD Regulation to exempt ICAC from Part 2 of the SD Act to permit it to obtain, possess, publish or communicate relevant material in accordance with the ICAC Act where that material was obtained by a third party using a surveillance device contrary to the SD Act. The exemption is to support a current and ongoing investigation by the ICAC and is due to expire on 31 December 2025.

The tension between ICAC's statutory remit and powers to investigate certain conduct on one hand, and ss 11, 12 and 14 of the SD Act on the other, is not unique to ICAC. There are a wide range of investigative bodies that may be hindered in their ability to discharge their statutory functions to investigate certain conduct or risks to persons, or handle complaints or reports about certain conduct or issues, by ss 11, 12 and 14 of the SD Act.

DCJ considers that exceptions should be included in ss 11 and 14 of the SD Act to permit any investigative bodies to communicate and publish material in accordance with their statutory powers and obligations.

---

[94] *Independent Commission Against Corruption and Ombudsman Legislation Amendment Act 2009*.

6.2.5.1 Thresholds and limitations for communication and publication by investigative bodies

Under privacy legislation public sector officials who work for investigative bodies are generally subject to statutory obligations in relation to the use and disclosure of information they obtain. These obligations are summarised in Appendix A. These obligations generally protect persons against their personal information being used and disclosed by investigative bodies unless the use or disclosure is connected to executing law enforcement or investigation functions. Also, under s 62 of the NSW Privacy Act, it is an offence for a public sector official, otherwise that in connection with the lawful exercise of his or her official functions, to intentionally disclose or use any personal information the official has had access to in the exercise of their official functions.

Many of the laws that investigative bodies operate under also impose restrictions on disclosure of information by persons who work for those bodies. For example, s 159 of the *Children's Guardian Act 2019* makes it an offence for a person to disclose information obtained in connection with the administration or execution of that Act unless the disclosure is made:

(a) with the consent of the person from whom the information was obtained, or
(b) in connection with the administration or execution of this Act or the regulations, or
(c) for the purposes of legal proceedings, or a report about legal proceedings, arising out of this Act or the regulations, or
(d) in accordance with a requirement imposed under the *Ombudsman Act 1974*, or
(e) with a lawful excuse.

Given that persons who work for investigative bodies are subject to statutory obligations and responsibilities, including in relation to the use and disclosure of information they obtain, DCJ considers that it is appropriate to exempt those persons from liability under s 11 and s 14 of the SD Act if they are communicating or publishing the illegal surveillance material in accordance with their statutory obligations.

DCJ does not consider it necessary to include a threshold requirement that communication or publication by investigative body employees be reasonably necessary in the public interest, or any similar requirement, because it can be assumed that it is in the public interest for those persons to exercise and act in accordance with the statutory powers and functions which Parliament has given them.

As noted above, some stakeholders raised concerns that exceptions to ss 11 and 14 may encourage law enforcement officers or regulatory officers to circumvent the warrant scheme in Part 3 of the SD Act and either use surveillance devices illegally, or induce third parties to use surveillance devices illegally, to obtain material that an investigative body can then use.

As discussed above in 6.2.1 and 6.2.2.3, there are other deterrents in the SD Act and under other laws to dissuade individual officers from deciding to use surveillance devices in breach of the SD Act. DCJ acknowledges however that it may be appropriate to draft the exception for use of illegal surveillance material by employees of an investigative body so as to disincentivise officers of such bodies to illegally use a surveillance device so that the investigative body may use the material obtained.

DCJ therefore proposes that the exceptions make clear that no employee or member of the investigative body will be able to use the illegal surveillance material if they know that a current or former employee of the body was in any way involved in the illegal use of a surveillance device to obtain the material.

One stakeholder raised that if public interest exceptions are introduced to ss 11 and 14, they will operate as defences. The onus will be on the accused to establish that an exception applies. DCJ notes that it would be difficult for a person to prove a negative, i.e. that no employee of the investigative body was in any way involved in the illegal use of the device.

DCJ also notes that investigative bodies may receive information provided anonymously or under a pseudonym. This is recognised for example in the PID Act, which provides that a voluntary public

interest disclosure may attract the protections in that Act even if is anonymous.[95] In such a case the employees of an investigative body may not be able to determine who was involved in the illegal use of the surveillance device which produced the material. DCJ does not consider it in the public interest for the investigative body employee to be precluded from using the material in such circumstances.

Accordingly, DCJ proposes that the exception be drafted so that a person who works for an investigative body should be permitted to communicate or publish illegal surveillance material in accordance with their statutory powers and obligations, **unless** the person knows that a current or former employee of the investigative body was in some way involved in the illegal use of the device which created the material, including causing another person to illegally use the device.

This will mean that the person will not need to be able to positively establish that no investigative body employees were complicit in the illegal surveillance that produced the material in order to use that material. However, if there is evidence that an employee **was** complicit in the illegal use, **and** the employee who communicates or publishes the material knows this, the latter person may be held liable under s 11 or 14. In practice drafting the exception this way will place responsibility under s 11 and s 14 on investigative bodies to ensure they have appropriate policies and practices in place to dissuade their employees from using surveillance devices illegally with the purpose of their employer then using the material.

6.2.5.2 Referral to other investigative bodies or prosecuting authorities

One stakeholder submitted that public interest exceptions to s 11 and s 14 should ensure that investigative bodies can disseminate illegal surveillance material to other investigative bodies if the latter is the more appropriate body to deal with the matter to which the material relates. The same stakeholder also noted that investigative bodies may need to be able to refer the material to prosecuting authorities if the investigating body itself is not able to initiate prosecutions.

DCJ agrees that it is appropriate to ensure that under the public interest exceptions the initial investigative body that receives illegal surveillance material can communicate or publish that material to a second investigative body, or refer the material to a prosecuting authority. This would permit for example, NSPWF to provide illegal surveillance material it receives about corrupt conduct to the ICAC, and for ICAC to refer the material on to the NSW Office of the Director of Public Prosecutions if it considers it appropriate.

The proposed exceptions should also clearly permit that second investigative agency or prosecuting authority which was referred the illegal surveillance material to communicate or publish the material in accordance with their statutory functions.

Recommendation 3 – Section 11 and section 14 of the SD Act should be amended to include an exception that the offences in those sections will not apply to communication or publication of illegal surveillance material:

- **by any person working in an investigative body or a prosecuting authority**
- **in accordance with their statutory functions and obligations**
- **to any person (including another investigative body or a prosecuting authority)**
- **unless the person who communicates or publishes the material knows that a current or former employee of the investigative body or prosecuting authority was involved in the surveillance device being used in breach of the SD Act to obtain the material, including causing another person to use the device illegally.**

[95] *Public Interest Disclosures Act 2022*, s 24(2)(b).

An example of the operation of the Recommendation 3 exceptions is illustrated in the flowchart on page 7.

6.2.5.3 Admissibility of illegal surveillance material

Some stakeholders raised questions in their submissions about how public interest exceptions to s 11 of the SD Act would affect the application of s 138 of the *Evidence Act 1995*. Section 138 provides that evidence that was obtained:

(a) improperly or in contravention of an Australian law, or

(b) in consequence of an impropriety or of a contravention of an Australian law,

is not to be admitted unless 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.

DCJ's proposed public interest exceptions to s 11 and s 14 of the SD Act will not undermine the application of s 138 of the *Evidence Act 1995*. A court will retain the discretion under s 138 to determine whether any illegal surveillance material which an investigating body or prosecuting authority seeks to admit as evidence in proceedings, or any evidence obtained as a consequence of that evidence, should be admitted into evidence.

In considering this issue it is instructive to refer to the case of *Kadir v the Queen*,[96] in which the High Court considered whether surveillance devices recordings obtained in breach of s 8 of the SD Act, and evidence obtained as a consequence of those initial breaches, should be admitted in a criminal prosecution for animal cruelty. The facts in that case are relevant as they highlight a type of scenario against which the effect of the public interest exceptions being proposed by DCJ can be considered.

In *Kadir*:

- Following an anonymous complaint of animal cruelty in relation to live baiting in greyhound racing on K's land, an animal welfare company Animals Australia hired a photographer to obtain surveillance evidence.
- The photographer unlawfully entered K's land on multiple occasions and covertly obtained seven video recordings in breach of s 8 of the SD Act (the surveillance evidence).
- Animals Australia then provided copies of the surveillance evidence to the RSPCA.
- RSPCA officers used the surveillance evidence in support of an application for a search warrant.
- The search warrant was granted, and when RSPCA officers executed the warrant on K's land, they seized further evidence of serious animal cruelty.
- The photographer also returned to K's property and engaged in conversations with K in which K allegedly made certain admissions.
- K was charged with acts of serious animal cruelty, and applied to have the surveillance evidence, the search warrant evidence and K's admissions excluded under s 138 of the *Evidence Act 1995*.

The High Court ultimately decided that the surveillance evidence should be excluded under s 138, but the search warrant evidence and Ks' admissions were admissible.

The High Court explained that s 138 'provides for the conditional exclusion of evidence obtained by, or in consequence of, impropriety or illegality in any proceeding to which the Act applies', and that 'the "discretion" conferred is to admit the evidence, should the court be persuaded that the balance of the competing public interests requires that outcome.'[97] The High Court confirmed that the

---

[96] *Kadir v the Queen* (2020) 267 CLR 109, 125.

[97] Ibid 125.

exclusion 'is not confined to evidence that is improperly or illegally obtained by police or other law enforcement agencies'.[98]

The High Court acknowledged the competing public interests informing s 138, stating:

> The desirability of admitting evidence recognises the public interest in all relevant evidence being before the fact-finding tribunal. The undesirability of admitting evidence recognises the public interest in not giving curial approval, or encouragement, to illegally or improperly obtaining evidence generally.[99]

The High Court confirmed that s 138:

> Does not enact the doctrine that prevailed in the United States, requiring the exclusion of the "fruit" of official illegality unless the impugned evidence was derived "by means sufficiently distinguishable to be purged of the primary taint". Section 138 provides for the exclusion of evidence obtained by, or in consequence of, impropriety or illegality, unless the product of balancing the competing public interests favours admitting the evidence.[100]

The High Court also confirmed that when considering under s 138 'the way in which the evidence was obtained' the court should consider the way the search warrant evidence and admissions were each obtained, separate to the way in which the surveillance evidence was obtained.[101] The High Court held that:

> The undesirability of receiving the search warrant evidence and the admissions, in the way each was obtained, materially differed from the undesirability of receiving the surveillance evidence in the way it was obtained.[102]

The High Court noted that:

> the surveillance evidence was obtained in contravention of the law by a private body (or persons engaged by it), whereas the search warrant evidence was obtained by a regulator acting lawfully and without prior knowledge of the contravention, albeit that it was procured on the strength of the surveillance evidence.[103]

The High Court concluded that an appropriate weighing of the public interests involved weighed in favour of the search warrant evidence being admitted under s 138, as:

> The admissibility of the search warrant evidence arises in criminal proceedings in which the desirability of admitting the evidence reflects the public interest in the conviction of wrongdoers. The undesirability of admitting evidence obtained in consequence of the deliberate unlawful conduct of a private "activist" entity is the effect of curial approval, or even encouragement, of vigilantism. The RSPCA had no advance knowledge of Animals Australia's plan to illegally record activities at the Londonderry property. There is nothing to suggest a pattern of conduct by which Animals Australia or other activist groups illegally collect material upon which the RSPCA takes action. The desirability of admitting evidence that is important to the prosecution of these serious offences outweighs the undesirability of not admitting evidence obtained in the way the search warrant evidence was obtained.[104]

DCJ's proposed public interest exceptions for s 11 and s 14 generally align with the reasoning of the High Court in *Kadir*. Under the proposed exceptions:

- Animals Australia and the photographer would remain criminally liable for the breach of s 8 of the SD Act, and also for a breach of s 12 because they were both complicit in the breach of s 8.
- Animals Australia would be permitted to communicate the surveillance material to the RSPCA (under the Recommendation 2 exception)

---

[98] Ibid 125.

[99] Ibid 134.

[100] Ibid 134 (citation omitted).

[101] Ibid 134.

[102] Ibid 134.

[103] Ibid 135.

[104] Ibid 137.

- RSPCA would be permitted to communicate and publish the surveillance material, including using it to apply for a search warrant, because RSPCA was not complicit in the photographer/Animals Australia obtaining the material in breach of s 8 (under the Recommendation 3 exception)
- RSPCA would be permitted to communicate the search warrant evidence as part of the prosecution of K (under the Recommendation 3 exception).

6.3 Exception to s 11 for communication and publication other than to/by investigative bodies

6.3.1 Arguments in favour of exceptions allowing publication of illegal surveillance material to any person

As noted in 4.3, a number of submissions supported an exception to s 11 and s 14 that would allow communication and publication of illegal surveillance material to any person if it is in the public interest. Some submissions also supported exceptions that would allow communication and publication to and by media organisations.

Those submissions that supported publication by and to any person and/or exceptions for media organisations submitted that broad publication of material, including by media organisations, can play a significant role in exposing wrongdoing and created public pressure for change. For example one stakeholder submitted that 'when unlawful animal cruelty is captured and reported to law enforcement authorities little to no action is taken so pressure from public exposure is needed'. Another stakeholder noted in their submission that publication of material is sometime necessary '[f]or policy and social change to occur, and for law reform to result', and that publication by media organisations can 'encourage public awareness, transparency and accountability, and law reform'.

Another stakeholder submitted that '[w]e rely on responsible journalism and freedom of communication to make sure the public is properly informed on matters of public interest', and provided examples from Victoria (which has a broad exception for publication of surveillance material in the public interest) such as:

- media reporting exposing the mistreatment of older people in aged care facilities and nursing homes, which included footage captured on hidden cameras, ultimately leading to the establishment of the Royal Commission into Aged Care Quality and Safety in 2018.
- media exposing acts of bestiality at a piggery captured on undercover footage, which led to changes to Victoria's bestiality laws.

That stakeholder submitted that 'media organisations in New South Wales are being forced to assume extraordinary legal risk and it is stifling their ability to report on matters of public importance'. The stakeholder submitted that an exception to s 11 should allow publication to and by any person, and should not be limited to publication to or by authorities, because:

- If a whistleblower has illegal surveillance material that raises serious concerns that are in the public interest but the material does not disclose any unlawful or corrupt conduct which can be investigated by an authority, 'it would be in the public interest for the whistleblower to be able to give the information to a reputable media outlet to report on the situation, which may even be a catalyst for changing laws or policies to ensure this conduct is made unlawful in the future'.
- if authorities have failed to act on information that has been reported to them 'it is clearly in the public interest for a journalist to be able to run a story on the failure of the authorities to act – including the original footage or information that was given to them', and
- 'many whistle-blowers are wary of authorities, or may have had difficulties themselves with the authorities in the past…Allowing other avenues such as journalism allows the journalist to inform

the authorities and provide them with the evidence should a member of the public be fearful to do so.'

The stakeholder however also submitted that the exception to s 11 should not be limited to media organisations, because:

- 'there are many reasons why a media organisation may choose not to run a story, even if it contains matters genuinely in the public interest, including because they simply do not have the time or resources, or because the matter pertains to a large advertiser with the media publication', and
- the stakeholder was concerned that the definition of 'media organisation' would not necessarily extent to digital media such as 'a website, a blog or a social media page – all of which can be sources of high-quality journalism'.

The stakeholder therefore submitted that another avenue, other than publication to and by authorities and media organisations, was necessary to ensure that public interest material was brought to light.

The stakeholder did not submit that an exception allowing publication by and to any person, and/or by and to a media organisation, was necessary for s 14 in relation to information obtained from a data surveillance device.

6.3.2 Arguments against allowing publication to and by media or any person

A number of stakeholder submissions opposed an exception to s 11 and s 14 of the SD Act allowing publication of illegal surveillance material to and by any person, or publication to and by media organisations, in the public interest. Stakeholders were concerned that such exceptions were too broad, and that they would encourage people, including media organisations, to trespass and to commit offences under ss 7, 8 and 9 of the SD Act. Some stakeholders raised concerns about the difficulties of regulating the media.

One stakeholder raised concerns that allowing any person to publish illegal surveillance material could result in people engaging in illegal surveillance and then publishing the material for personal or political gain, noting that while media organisations are subject to codes of conduct, the same is not true of members of the community who can publish information through social media. The stakeholder submitted that:

> when surveillance devices are used illegally, and the resulting information is freely shared without restriction, the crucial balance between privacy rights and the public's right to know becomes almost impossible to achieve.

That stakeholder also submitted that media organisations may be biased towards releasing information due to their own commercial and other underlying interests, and therefore supported the requirement for an order for a judge before media organisations could publish illegal surveillance information.

Other stakeholder submissions also raised concerns about the privacy implications if any person was permitted to publish illegal surveillance material to the world at large. One stakeholder raised particular concerns about risks to privacy and online safety that might arise or be amplified if the material was published online.

Another stakeholder submission raised concerns about consequences for the privacy and safety of victims, and particularly victims of domestic violence, if publication by or to any person was permitted. The stakeholder noted that:

> there may be limited circumstances, for example involving domestic and family violence considerations or situations where apprehended violence orders are in place, where the safety and protection of vulnerable parties must take precedence.

This linked in with the concerns raised by a different stakeholder, discussed in 6.2.4.2, that if the illegal surveillance material related to an act of sexual violence, the consent of the victim should be required before the material is shared with police (that stakeholder did not support an exception permitting publication to the world at large).

Another stakeholder submitted that if publication to the world at large was permitted, consideration would need to be given to imposing limits on the type of content that could be published, for example prohibiting publication if the illegal surviellance material featured a person in a vulnerable group, such as NDIS participants.

Another stakeholder submitted that exceptions allowing publication to and by media organisations in the public interest were unnecessary because the PID Act and the Corp Act both provide protections for whistleblowers, including when they disclose certain conduct to the media (provided certain requirements are met – see 5.2 above).

6.3.3 DCJ discussion and conclusion

DCJ acknowledges that publication to the world at large about serious wrongdoing, particularly publication by media organisations, can be an important mechanism to create public pressure for accountability and for changes to law and policy.

DCJ notes that under the Recommendation 2 exceptions and the Recommendation 3 exceptions there are pathways that would permit publication of illegal surveillance material by an investigating body, if a person chooses to provide the material to an investigating body, or the investigative body requires the person to provide it, and that body determines it is appropriate, in accordance with its statutory obligations and responsibilities, to publish the material.

DCJ acknowledges that even when an avenue is available for such information to be provided to investigative bodies, there may still be a public interest in that information being made public, including if the bodies fail to act. This is reflected, for example, in the provisions in the PID Act and the Corp Act that provide that if a public official discloses information to a relevant authority but that authority fails to act in a timely manner to address the wrongdoing, the public official is permitted to disclose information to an MP or the media (under the PID Act and Corp Act), or to any person (under the Cth PID Act) (see 5.2).

DCJ notes however that each of those Acts only permit whistleblowing by public officials, or, in the case of the Corp Act, employees or contractors. Also, each of those Acts provides a comprehensive framework for whistleblowing which includes obligations for agencies that can receive disclosures. These frameworks include timeframes for when, in effect, it is reasonable for the person who made the disclosure to conclude that the agency to which they disclosed the material has not dealt with it effectively (6 months under the PID Act, 90 days under the Cth PID Act and Corp Act).[105] These timeframes may not be appropriate for all disclosures of illegally obtained surveillance device material provided to law enforcement, integrity and regulatory agencies.

DCJ also notes the risk that a person who has provided material to an investigating body and then publishes that material may inadvertently jeopardise an ongoing investigation.

DCJ also acknowledges that, as some stakeholders have noted, there may be significant public interest in information about harmful conduct that is not illegal, and does not come within the remit of any particular investigative body, being able to be brought to light in support of an argument that there is a need for the law to address such behaviour.

However, a key consideration is that the material that s 11 of the SD Act is concerned with was obtained illegally, either by a person listening to or recording a private conversation without consent

---

[105] *Public Interest Disclosures Act 2022 (NSW),* s 28; *Public Interest Disclosures Act 2013* (Cth) s 52; *Corporations Act 2001* (Cth), s 1317AAD(1).

of the parties involved, or trespassing on a person's property, or tracking a person's location without their consent. Similarly, s 14 of the SD Act is concerned with information that was obtained by a person monitoring information going in and out a person's computer without the consent of the person in lawful possession or control of the computer.

DCJ notes that the equivalent offences to s 11 of the SD Act in the other Australian jurisdictions which have public interest exceptions are broader than s 11. This is because they are structured to prohibit communication and publication of **both legal and illegal** surveillance device material concerning private conversations and private activities, and then provide for exceptions. The fact that s 11 of the SD Act **only** criminalises communication and publication of illegal surveillance material means the balance of competing public interests to be achieved when creating exceptions to s 11 is necessarily different.

Publication of illegal surveillance material also itself constitutes an invasion of the privacy of persons depicted in the material, unless those persons have consented. The ease with which information can be shared online by any person through social media means the extent of the invasion can multiple exponentially.

A person who receives illegal surveillance material must make an important ethical calculation as to whether, in the particular circumstances, the public interest in that material being published outweighs the public interest in a person's privacy being protected, and the public interest in not encouraging or incentivising criminal behaviour.

One option would be to require a judge to make this calculation by the exception requiring an order from a judge to permit publication. However, as discussed above in 4.2.3, the clear majority of stakeholders did not support a requirement for a judicial order before permitting communication or publication. Stakeholders submitted that such a requirement would be onerous, costly and time consuming and may cause delays in preventing or addressing harmful conduct.

Another option could be to provide an exception under s 11 of the SD Act to permit a person to provide the illegal surveillance material to an MP or journalist, if reasonably necessary in the public interest, as is the case under the PID Act. This option could address concerns from stakeholders that illegal surveillance material that relates to a matter of public interest should be able to be disclosed beyond investigative bodies, if reasonably necessary, for example if the investigating body has failed to act on the material provided, or if the matter of public interest is not within the jurisdiction of any investigative body.

However, DCJ considers that at this point in time, the potential risks of encouraging invasions of privacy associated with an exception to s 11 allowing communication and publication of illegal surveillance material in these circumstances outweigh the potential benefits. The changes proposed above in this report to permit communication and publication of illegal surveillance material to and by investigative bodies would be a significant development of the current law. It would be prudent to first implement those changes and then allow an adequate amount of time to observe and evaluate the impact of those changes before considering broader reform.

DCJ proposes below that there should be a requirement for a statutory review of the amendments proposed in this report 5 years after the amendments have commenced (see 6.5.1 and recommendation 6). The statutory review could consider whether an exception should be introduced into s 11 of the SD Act to permit communication and publication of illegal surveillance material to persons and organisations other than investigative bodies in the public interest.

The Minister conducting the statutory review will be in a position to consider the type of material that is provided to investigating bodies in reliance on the exceptions proposed in this report, and whether there is a need for further law reform because of investigative bodies failing to act on relevant material, or certain important material falling outside the remit of any investigative body.

Finally, DCJ considers that it would not be appropriate to create an exception to **s 14** of the SD Act to permit persons to provide information about the input or output of another person's computer, obtained by illegally using a **data surveillance device**, to MPs or journalists in the public interest. The

definition of a data surveillance device, and the circumstances in which use of such a device will be illegal under s 10 of the SD Act, are discussed in 6.2.3.

No other jurisdiction has a public interest exception for publication and communication of information from a data surveillance device. Further, stakeholders' submissions did not provide any examples of when communicating or publishing illegal surveillance material from a data surveillance device beyond investigative bodies would be necessary in the public interest.

6.4 Other related exceptions to s 11 and s 14

6.4.1 Republication of illegal surveillance material

A stakeholder raised concerns that if a member of the public uses their social media account to share an online media article that reports on information derived from an illegal use of a surveillance device, the person (and others on social media who share the article) may be in breach of s 11 of the SD Act. This stakeholder submitted that exceptions were needed to ensure that 'we do not have situations where people are inadvertently or innocently found to be in breach of the SD Act'.

DCJ agrees that a person should not be criminalised for sharing illegal surveillance material that has been lawfully published by an investigating body in accordance with the exceptions proposed by DCJ in this report. DCJ also considers that it is not appropriate to expect that members of the public will be able to identify whether material has been published lawfully under s 11 or s 14 of the SD Act or any other legislation before choosing whether to re-publish it.

DCJ also considers it important to ensure that once information has been lawfully published under either framework mentioned above, media organisations should be able to re-publish and comment on the published content.

DCJ recommends that an exception be included in s 11 and s 14 to provide that it is not an offence for a person to communicate or re-publish illegal surveillance material that has already been published to the world at large, unless the person knows the initial publication of the material was in breach of s 11 or 14 of the SD Act.

The flowchart on page 7 illustrates how this proposed exception will operate with the other proposed exceptions to the SD Act.

Recommendation 4 – Section 11 and s 14 of the SD Act be amended to insert exceptions which provide that it is not an offence under those section for a person (the re-publisher) to communicate or re-publish illegal surveillance device material that another person or body has already been published to the world at large, unless the re-publisher knows the original publication of the material was in breach of s 11 or 14 of the SD Act.

6.4.2 Communication to lawyers or health care professionals

One stakeholder submitted that exceptions to s 11 should permit dissemination of illegal surveillance material to legal representatives for the purposes of obtaining legal advice. Another stakeholder raised concerns that the offences in the SD Act may prevent victims sharing illegally-obtained surveillance device material with health-related bodies in order to seek support for health and wellbeing such as counselling.

While DCJ agrees that neither of these scenarios should attract criminal liability, for practical reasons DCJ does not consider it necessary to include separate exceptions to s 11 or s 14 of the SD Act to specifically exclude these scenarios. Firstly, both lawyers and health professionals operate on the basis of confidentiality of communications with their clients. Lawyers and health professionals would be breaching this professional confidence if they reported to police about the communication of the material by their client.

In the unlikely scenario that the professional (or a third party who somehow discovered the dissemination) did report to police, the police would need to seek the Director of Public Prosecution's approval to prosecute the client,[106] and the DPP would need to approve the prosecution as being in the public interest. It is difficult to imagine a scenario in which the DPP would consider it in the public interest to pursue a prosecution against a person for sharing illegal surveillance material with their lawyer or health-professional for the purpose of receiving advice or support.

6.5 Other issues and recommendations from stakeholders

6.5.1 Requirement for a statutory review

Some stakeholder submissions recommended that there be a review of the operation of any public interest exceptions added to ss 11, 12 or 14 of the SD Act within 5 years of the commencement of the exceptions.

DCJ agrees that it would be appropriate for there to be a statutory review of the operation of the exceptions proposed in this report, to ensure that the exceptions are operating as intended, and to consider if any further amendments are needed. DCJ also agrees that five years is an appropriate point at which to commence such a review. If any shorter period is set for review there is a significant risk that there will not be sufficient data to assess the operation of the exceptions, as the SD Act offences are not frequently charged.

Recommendation 5 – The SD Act be amended to include a requirement that the Minister commence a statutory review of the amendments proposed in this report as soon as practicable after 5 years after the commencement of the amendments.

6.5.2 Disclosure in response to a subpoena

One stakeholder submitted that DCJ should consider circumstances where possession, communication or publication of illegal surveillance material may be authorised or required by subpoena or search warrant or other type of NSW statutory instrument, and noted that the NSW Privacy Act permits public sector agencies to disclose personal information in those circumstances.[107]

Disclosure of illegal surveillance material under a search warrant will be covered by the Recommendation 2 exceptions. In relation to production in response to a subpoena, the stakeholder did not provide any information as to whether there is a need to change the law in this regard. It is unclear whether the fact that compliance with a subpoena may cause a person to be in breach of s 11 or 14 of the SD Act is a basis on which subpoenas are being resisted. DCJ considers that without more information from stakeholders on this point, a change in the law is not justified at this time. If evidence emerges that there is a problem in this regard, the issue can be considered as part of the statutory review.

6.5.3 Changes to other parts of the SD Act

Some stakeholders submitted that parts of the SD Act other than ss 11, 12 and 14 are out of date and require review and amendment.

---

[106] See 2.2 above which discusses the requirement for the consent of the Director of Public Prosecutions to commence proceedings for an offence under the SD Act.

[107] *Privacy and Personal Information Protection Act 1998* s18(c) and s 235(c).

One stakeholder submitted that the definitions of 'listening device' and 'optical surveillance device' in s 4 of the SD Act are out of date as they refer to exclusions of devices that are used by someone with impaired hearing or impaired vision to 'overcome the impairment'.

The stakeholder suggested that the following amendments to the definitions:

- The definition of a listening device provide that it does not include 'an assistive hearing device used as a disability aid by a person who is deaf or hard of hearing.'
- The definition of an optical surveillance device provide that it does not include 'a device designed to be used by a person who is blind or has low vision to assist with vision'.

The definitions of listening device and optical surveillance device in s 4 of the SD Act were taken from the model legislation for surveillance device laws which was published in 2003 by the Standing Committee of Attorneys-General and Australasian Police Ministers Council Joint Working Group on National Investigation Powers.[108]

DCJ acknowledges that the language in the definitions of 'overcoming impairment' is out of date and may be offensive to persons with disability, and agrees that this language should be replaced. However further consultation with stakeholders will be necessary to ensure that the language that is used to replace the outdated references is in accordance with the most current standards, and that it does not inadvertently change the scope of the definitions, and therefore the scope of the offences in ss 7-10 of the SD Act.

DCJ will consider this stakeholder proposal further outside of this consultation.

The same stakeholder also suggested that the offence in s 7 of the SD Act for using a listening device should be amended to 'clarify that an interpreter, despite not being a participant in a private conversation, is privy to that conversation and their consent should be obtained in the same manner as those participants' consent.' This could potentially change the scope of the offence in s 7 of the SD Act for using a listening device, and such a change which falls outside the parameters of this consultation. The stakeholder did not provide any examples or further detail that illustrate why this change may be necessary. Without further information DCJ does not consider this change is justified at this time.

One stakeholder submitted that DCJ should consider:

- revising the title and objects of the SD Act ' to underscore the paramount importance of balancing matters of public interest and ensuring that the privacy of individuals is not unnecessarily impinged upon by providing strict requirements around the installation, use and maintenance of surveillance devices'. The submission does not provide a reason why the title of the SD Act should be amended. In relation to the objects, DCJ does not consider any changes are needed, as the objects only refer to the use of surveillance devices, not the use of the material obtained from use of surveillance devices.
- 'if further reforms are required to ss 7 to 10 of the SDA as a corollary to this process'. DCJ has considered the relationship between the offences in ss 7-10 of the SD Act and the offences in ss 11, 12 and 14 of the SD Act throughout this report and when making recommendations. Reviewing the scope of the offences in ss 7-10 falls outside the scope of this consultation, and would require a detailed separate consultation to ensure that any changes did not have unintended consequences.

Another stakeholder submitted that the SD Act:

> needs to be modernised as befits a statutory instrument attempting to regulate behaviour in a context where technological development has outstripped the capacity of the law to deal with it several times over in the 17 years since its commencement… Listening devices and optical surveillance devices as

[108] Standing Committee of Attorneys-General and Australasian Police Ministers Council Joint Working Group on National Investigation Powers, *Cross-Border Investigative Powers for Law Enforcement* (Report, November 2003), p 362-364.

> described in this legislation are no longer capable of capturing the technological capacity or covering the field of potential technological incursion into modern life.

The stakeholder submitted that 'piecemeal amendment risks missing the more significant issues with aged legislation and may create unintended consequences'.

A wholesale review of the SD Act would require significant resources and significant further consultation with stakeholders. The amendments proposed in this report are modest proposals which will ensure a more appropriate balance between competing public interests is struck in ss 11, 12 and 14 of the SD Act without fundamentally changing the intent of the SD Act.

6.5.4 Changes to other Acts

A number of submissions, including the campaign submissions, submitted that public interest exceptions permitting communication and publication of illegal surveillance material under the SD Act should 'override' the powers of authorities under the Biosecurity Act to seize material. Such submissions submitted that '[r]obust safeguards are needed to prevent the misuse of biosecurity laws to suppress evidence of wrongdoing' and one stakeholder further submitted that:

> law enforcement and other authorities should be prohibited from seizing material of relevance to the public interest in contravention of the SDA where that seizure prevents an intended communication or publication of the material.

Some submissions recommended that there need to be comprehensive whistleblower protections within the SD Act. A stakeholder submitted that the exceptions in the SD Act need to 'afford comprehensive protections to whistleblowers', including protection against prosecution under other Acts such as the Biosecurity Act. Another stakeholder similarly submitted that there should be 'robust' protections for whistleblowers under the SD Act and the 'establishment of clear legal safeguards to shield individuals who engage in such activities'. The same stakeholder submitted that the NSW Government should:

> undertake a legislative review and harmonisation process which includes legislative audit and review of existing State and Commonwealth legislation such as laws related to privacy, whistleblower protection, defamation and other relevant statutes....[and amend] any conflicting provisions identified in the audit and review process to align with the public interest exceptions in the SDA.

DCJ does not consider that the SD Act is the appropriate legislative vehicle in which to design a permissive whistleblowing scheme. The focus of this consultation is on removing criminal liability under the SD Act when a person provides information based on illegal surveillance on to investigative bodies appropriately in the public interest. As discussed in 5.2, there are a range of other NSW and Commonwealth which contain permissive whistleblowing provisions and provide protection from criminal liability for whistleblowers who meet the criteria in those Acts. The amendments proposed in this report will ensure that those whistleblower protections in other laws are not undermined by ss 11, 12 and 14 of the SD Act.

In relation to the submissions from stakeholders regarding the seizure powers under the Biosecurity Act, DCJ notes that that Act authorises the appointment of 'authorised officers' with powers to enter premises and investigate potential breaches of the Act, including the power to seize any thing the authorised officer believes on reasonable grounds is connected with an offence against the Biosecurity Act or regulations.[109]

There are safeguards in the Biosecurity Act if an authorised officer seizes an item, namely:

- the authorised officer is required to provide a receipt for the thing seized.[110]

[109] *Biosecurity Act 2015*, s 98 and s 102(2)(p).

[110] *Biosecurity Act 2015*, s 106.

- The authorised officer must return the seized thing to its owner if satisfied that it is lawful for the owner to have possession of the thing, and the continued retention of the thing in custody is not justified.[111]
- Any person can apply to a court for an order directing that a seized thing be delivered to the person, and the court may make such an order if satisfied that the person is the owner of the seized thing, it is lawful for the person to have possession of the thing, and the continued retention of the seized thing in custody is not justified.[112]

DCJ concludes that if stakeholders consider that further safeguards are needed in relation to the seizure powers, the Biosecurity Act, rather than the SD Act, would be the appropriate place for such amendments.

[111] *Biosecurity Act 2015*, s 107(1).

[112] Biosecurity Act 2015, s 109.

7 Appendix A – Obligations imposed by privacy legislation

7.1 *Privacy Act 1988* (Cth)

The *Privacy Act 1988* (Cth) (**Cth Privacy Act**) imposes duties on Australian Government agencies, private organisations (including corporations and sole traders) with an annual turnover of more than $3 million, and certain small business operators (referred to as '**APP entities**'). The Cth Privacy Act does not cover an individual acting in a personal capacity.[113]

The Cth Privacy Act contains 'Australian Privacy Principles' (**APPs**) which are legal duties that apply when handling personal information. Personal information includes video or audio footage of a person from which that person can reasonably be identified. The duties in the APPs relate to the collection, storage, use and disclosure of that personal information.[114] Most relevantly, the Cth Privacy Act imposes duties on APP entities generally to:

- only collect personal information that is reasonably necessary for the organisation's functions or activities (APP 3)
- if the APP entity receives personal information it did not solicit, determine whether it could have collected the personal information and if not, to de-identify or destroy the information and otherwise to comply with the APPs as if the entity had collected the information (APP 4)
- not use or disclose the personal information for a purpose other than the primary purpose for which it was collected unless certain exceptions apply, including:
    - the person the information relates to has consented
    - the person the information relates to would reasonably expect the APP entity to use or disclose the information for the secondary purpose and that purpose is related to the primary purpose
    - the use or disclosure is required or authorised by or under an Australian law or a court or tribunal order
    - the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body (APP 6).

The definition of an 'enforcement body' in the Cth Privacy Act includes any agency 'to the extent that it is responsible for administering, or performing a function under, a law that imposes a penalty or sanction or a prescribed law'.[115]

The Cth Privacy Act also includes an exemption for media organisations. Section 7B(4) provides that an act or practice of a media organisation is exempt from the Cth Privacy Act if the act or practice is in the course of journalism and the organisation is publicly committed to observe published standards that deal with privacy in the context of the activities of a media organisation.

---

[113] *Privacy Act 1988* (Cth) s 7 (1) (ee) and 7B(1).

[114] *Privacy Act 1988* (Cth), sch 1.

[115] *Privacy Act 1988* (Cth), s 6.

The Cth Privacy Act contains civil penalties for APP entities that breach a person's privacy, for example by breaching an APP. The maximum penalties are:

- for a serious interference with privacy by a corporation - $50 million (s 13G(2))
- for a serious interference with privacy by an individual or other organisation - $2.5 million (s 13G(3))
- for an interference with privacy – 2,000 penalty units (s 13H(3)).

The Cth Privacy Act also gives the Australian Information Commissioner the power to make a determination that an APP entity's breach of an APP is permitted if the public interest in the entity engaging in an act or practice in breach of the APP outweighs the public interest in the entity adhering to the APP.[116]

7.2 *Privacy and Personal Information Protection Act 1998* (NSW)

The *Privacy and Personal Information Protection Act 1998* (**NSW Privacy Act**) imposes conditions and restrictions on NSW public sector agencies' collection, use and disclosure of 'personal information'. The Privacy Act contains 'Information Protection Principles' (**IPPs**) which are similar to the APPs in the Cth Privacy Act, relating to the collection, storage, use and disclosure of that personal information. Most relevant to this consultation, the NSW Privacy Act imposes duties on any NSW public sector agencies to:

- only collect personal information for a lawful purpose that is directly related to the agency's function or activities, and only where it is reasonably necessary for that purpose (s 8)
- take reasonable steps to ensure the information collected is relevant to the purpose for which is collected, and is not excessive, and the collection of the information does not intrude to an unreasonable extent on the personal affairs of the person to whom the information relates (s 11).
- only use the personal information for the purpose for which it was collected or a directly related purpose, unless the person to whom the information relates agrees to its use for another purpose, or the use is to prevent or lessen a serious or imminent threat to any person's health or safety (s 17)
- only disclose the personal information with the consent of the person to whom it relates (s 26(2), or
    - if the disclosure is directly related to the purpose for which the information was collected, and the agency disclosing the information has no reason to believe that the person concerned would object to the disclosure, or
    - the person concerned is reasonably likely to have been aware, or has been made aware at the time of collection, that information of that kind is usually disclosed, or
    - if the agency believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person (s 18).

These duties in the NSW Privacy Act generally would apply to NSW public sector agencies using surveillance devices to make recordings of persons and using and disclosing those recordings. However, the Privacy Act contains significant exemptions for law enforcement agencies,[117]

[116] *Privacy Act 1988* (Cth) s 72.

[117] *Privacy and Personal Information Protection Act 1998,* s 23(1) and s 27.

investigative agencies[118] and public sector agencies collecting, using or disclosing the information for legal proceedings or law enforcement purposes.[119] Generally speaking, these exceptions allow these agencies to collect, use and disclose personal information under the Act if it is necessary for law enforcement purposes, or, in the case of investigative agencies, if it is necessary in the exercise of the agency's complaint handling or investigative functions.

Section 62(1) the NSW Privacy Act also makes it **an offence** for a public sector official, otherwise than in connection with the lawful exercise of his or her official functions, to intentionally disclose or use any personal information about another person to which the official has or had access in the exercise of his or her official functions. The offence is punishable by up to two years' imprisonment or 100 penalty units, or both.

Under the NSW Privacy Act the NSW Privacy Commissioner may, with the approval of the Minister, make a determination that an NSW public sector agency is exempt from complying with an IPP if the Commissioner is satisfied that the public interest in the agency complying with the IPP is outweighed by the public interest in the Commissioner making the direction.[120]

Agencies' obligations under the NSW Privacy Act sit alongside the provisions of the SD Act. NSW public sector agencies must comply with both pieces of legislation. The exceptions for law enforcement and investigative agencies in the NSW Privacy Act do not alter the application of the offences in the SD Act.

7.3 *Health Records and Information Privacy Act 2002* (NSW)

The *Health Records and Information Privacy Act 2002* (**Health Privacy Act**) applies to all NSW public sector agencies, private sector persons and corporations (with an annual turnover of more than $3 million) that collect, hold or use health information. Health information includes any personal information (including audio and video footage) about the physical or mental health or a disability of an individual, or an individual's express wishes about the future provision of health services to him or her, or a health service provided, or to be provided, to an individual.[121]

The 15 Health Privacy Principles (**HPPs**) in the Health Privacy Act for the collection, use and disclosure of health information are substantially similar to the IPPs in the NSW Privacy Act. The Health Privacy Act also makes it a criminal offence, punishable by up to 2 years' imprisonment, for a public sector official to intentionally disclose or use any health information about an individual to which the official has or had access in the exercise of his or her official functions, otherwise than in connection with the lawful exercise of his or her official functions.[122]

The Health Privacy Act contains specific exemptions for certain specified law enforcement agencies.[123] The HPPs in the Health Privacy Act in relation to use and collection of health information also include exceptions for 'law enforcement' and 'investigative agencies' which permit use of health information for a secondary purpose if reasonably necessary for the exercise of the

[118] *Privacy and Personal Information Protection Act 1998* s 24. The definition of investigative agencies is broad and includes any public sector agency with investigative functions 'if those functions are exercisable under the authority of an Act or statutory rule…and the exercise of those functions may result in the agency taking or instituting disciplinary, criminal or other formal action or proceedings against a person or body under investigation': *Privacy and Personal Information Protection Act 1998* s 3.

[119] *Privacy and Personal Information Protection Act 1998* s 23 sub-ss (2)-(6A).

[120] *Privacy and Personal Information Protection Act 1998* s 41.

[121] *Health Records and Information Privacy Act 2002*, s 6.

[122] *Health Records and Information Privacy Act 2002,* s 68(1).

[123] Section 17 provides that the Health Privacy Act does not apply to ICAC, the NSWPF, the ICAC Inspector, LECC, the Inspector of LECC, or the NSW Crime Commission, except in connection with the exercise of their administrative and educative functions.

respective agencies' functions.[124] However, the term 'investigative agencies' is defined more narrowly than under the Privacy Act.[125] The Health Privacy Act also includes exceptions for news media. Section 15 of the Health Privacy Act provides that the HPPs in relation to collection, use and disclosure of health information do not apply to a news medium collecting, using and disclosing health information in connection with its new activities.

In terms of the relationship between the Health Privacy Act and the SD Act, s 18 of the Health Privacy Act expressly provides that an exemption from a HPP in the Health Privacy Act does not authorise an organisation (including a private individual) to do any thing that is otherwise prohibited under another Act or law. This means, for example, that a news organisation that is exempt from the restrictions on disclosure of health information under the Health Privacy Act will still be criminally liable under s 11 of the SD Act if the organisation discloses recordings containing health information which were recorded using a surveillance device in breach of ss 7 or 8 of the SD Act.

[124] *Health Records and Information Privacy Act 2002*, sch 1 ss 10 and 11.

[125] *Health Records and Information Privacy Act 2002*, s 4.

8 Appendix B – Whistleblower protections for members of the public

NOTE: This table includes examples of provisions in Acts which provide **protection from criminal liability** for **voluntary** complaints or disclosures from members of the public to a relevant agency. The below is not an exhaustive list of all Acts which may contain such provisions. Also, the below Acts, and other Acts, may contain different protections for persons who are **required or requested** by the agency to provide the information.

Who can the disclosure be made to	What disclosures will attract protections	Whistleblower protections from liability	Protections against detrimental or reprisal actions
Independent Commission Against Corruption (ICAC) (*Independent Commission Against Corruption Act 1988*)	Information about a matter that concerns or may concern **corrupt conduct** (s 79D) (corrupt conduct is defined in ss 7-9, and necessarily involves a **connection with the conduct of by a NSW public official**)	Protection from **criminal, civil and disciplinary liability** for act of disclosing (s 79O) Attorney General may give undertaking that disclosure of past illegal conduct as part of whistleblowing will not be used in evidence in criminal or civil proceedings (s 79P)	Offence for person to take detrimental action against discloser (s 79I) Discloser can sue for damages if detrimental action taken (s 79J) Supreme Court can grant injunction to prevent or cease detrimental action (s 79L)
Law Enforcement Conduct Commission (LECC) (*Law Enforcement Conduct Commission Act 2016*)	Information that assists the LECC about conduct that concerns or may concern **serious wrongdoing** (s 97C) **by a member of the NSWPF or the NSW Crime Commission** (s 35)	Protection from **criminal, civil and disciplinary liability** for act of disclosing (s 97N) Attorney General may give undertaking that disclosure of past illegal conduct as part of whistleblowing will not be used in	Offence for person to take detrimental action against discloser (s 97H) Discloser can sue for damages if detrimental action taken (s 97I)

Who can the disclosure be made to	What disclosures will attract protections	Whistleblower protections from liability	Protections against detrimental or reprisal actions
	(Serious wrongdoing is defined in s 13 of the PID Act. It includes **corrupt conduct** (as defined in ICAC Act). It also includes '**serious maladministration**' which in turns is defined to include **conduct relating to administration that is unlawful, unreasonable, unjust, oppressive or improperly discriminatory.)**	evidence in criminal or civil proceedings (s 970)	Supreme Court can grant injunction to prevent or cease detrimental action (s 97K)
NSW Ombudsman (*Ombudsman Act 1974*)	Information about conduct that concerns or may concern **serious maladministration** (s 31M) **by a public authority** (s 12), subject to certain exceptions for certain authorities (Schedule 1) and certain matters (s 3M(1)(d) and (e)). (Serious maladministration is defined in s 13 of the PID Act (see above comments re disclosures to the LECC)).	Protection from **criminal, civil and disciplinary liability** for act of disclosing (s 31X) Attorney General may give undertaking that disclosure of past illegal conduct as part of whistleblowing will not be used in evidence in criminal or civil proceedings (s 31Y)	Offence for person to take detrimental action against discloser (s 31R) Discloser can sue for damages if detrimental action taken (s 31S) Supreme Court can grant injunction to prevent or cease detrimental action (s 31U)
Children's Guardian (*Children's Guardian Act 2019*)	Complaints about the **response of the head of a relevant agency to a report of:** • a **sexual offence or sexual misconduct in relation to a child,**	Protection from **criminal and civil liability** and any **liability arising by way of administrative process**, including disciplinary action, for giving the complaint (s 68)	Offence for person to take detrimental action against the complainant (s 64)

Who can the disclosure be made to	What disclosures will attract protections	Whistleblower protections from liability	Protections against detrimental or reprisal actions
	• **ill-treatment, neglect or assault of a child,** or behaviour that causes **significant emotional or psychological harm to a child.** • An offence relating to **failure to report to police or to reduce or remove a risk of child abuse** (s 28, and see definitions in Pt 4 Div 2).	If the complainant gives the Children's Guardian information or a document as part of their complaint, evidence of the information or document, and other evidence directly or indirectly derived from the information or document, is not admissible against the individual in a proceeding to the extent it tends to incriminate the individual, or expose the individual to a penalty, in the proceeding (S 69)	
Secretary of the Department of Communities and Justice **or** **An institution engaging in child-related work** *(Children and Young Persons (Care and Protection) Act 1998)*	A report about a child or young person (or a class of children or young persons) who the person has reasonable grounds to suspect is at risk of significant harm (s 24 and s 29AAA)	Making a report in good faith to the Secretary or a person who has the power or responsibility to protect the child or young person does not constitute a ground for civil or criminal liability against the person making the report (s 29) Making a report in good faith to the institution about a child or young person the person reasonably suspects is at risk of significant harm does not constitute a ground for civil or criminal liability against the person making the report (s 29AAA)	Offence for person to take detrimental action against the complainant (s 29AB)

Who can the disclosure be made to	What disclosures will attract protections	Whistleblower protections from liability	Protections against detrimental or reprisal actions
NSW Ageing & Disability Commissioner (*Ageing and Disability Commissioner Act 2019*)	A report about an **adult with disability or an older adult** the reporter has reasonable grounds to believe is **subject to or at risk of abuse, neglect or exploitation**, or about circumstances the discloser has reasonable grounds to believe will result in the abuse, neglect or exploitation of an adult with disability or older adult (s 13(1)).	Protection from **criminal and civil liability** and any **disciplinary action**, for making the report provided the reporter was acting in good faith (s 13(4))	None
National Disability Insurance Agency **or** **NDIS Quality and Safeguards Commissioner** (*National Disability Insurance Scheme Act 2013* (Cth))	Information the discloser suspects on reasonable grounds indicates that **an NDIS provider has, or may have, contravened a provision of the Act**, provided the discloser provides their name and makes the disclosure in good faith. (s 73ZB(2)).	The person is not subject to any **civil or criminal liability** for making the disclosure; and **no contractual or other remedy** may be enforced, and no contractual or other right may be exercised against the person on the basis of the disclosure. (s 737B)	Offence for person to take detrimental action ('victimisation') against the discloser (s 73ZC) Discloser can sue for compensation if detrimental action taken (s 73ZD)
National Anti-Corruption Commissioner or **Inspector-General of Intelligence and Security** (*National Anti-Corruption Commission Act 2022* (Cth))	Information about a corruption issue (s 23) (a corruption issue is that a person has engaged, is engaging or will engage in corrupt conduct, and corrupt conduct is defined in s 8 and necessarily involves a **connection with the conduct of a Commonwealth public official**)	Protection from **civil, criminal or administrative liability** (including disciplinary action) for the disclosure (s 24 and see s 27)	Offence for person to take detrimental action against the discloser (s 30)

Communities and Justice

NSW GOVERNMENT