Project Hakea

Criminal use of tracking and other surveillance devices in NSW

June 2024

New South Wales
Crime Commission

NSW GOVERNMENT

Published by the New South Wales Crime Commission

Project Hakea: Criminal use of tracking and other surveillance devices in NSW

First published June 2024

Acknowledgement of country

The New South Wales Crime Commission acknowledges the Traditional Custodians of the lands where we work and live. We celebrate the diversity of Aboriginal peoples and their ongoing cultures and connections to the lands and waters of NSW.

We pay our respects to the Elders, past, present, and emerging and acknowledge the Aboriginal and Torres Strait Islander people that contributed to this investigation.

Content warning and support

This report contains information that may be distressing to readers, including accounts of violence and abuse. If you or someone you know is experiencing domestic violence, there are a range of support services available, including 1800RESPECT (1800 737 732), the NSW Domestic Violence Line (1800 656 463), Lifeline (13 11 14), and 13YARN (13 92 76). In an emergency, always call Triple Zero (000).

Acknowledgements

The Commission would like to acknowledge the significant contribution and support provided by the NSW Police Force, including the Security Licensing & Enforcement Directorate, the Domestic and Family Violence Registry, and specialist squads within the State Crime Command. We also acknowledge the valuable assistance provided by the NSW Bureau of Crime Statistics and Research, the NSW Domestic Violence Death Review Team, the Australian Federal Police, the Department of Home Affairs, the Australian Transaction Reports and Analysis Centre (AUSTRAC), and those private organisations and individuals who shared their unique insights.

Contents

Executive Summary

Tracking devices are a growing enabler of serious and organised crime in NSW. Accessible, inexpensive, and easily concealed – they are used by organised crime networks (OCNs) to monitor, locate, and ultimately attack their rivals.

While tracking devices have been used in organised crime for over two decades, in recent years, the NSW Crime Commission (the Commission) has observed a sharp rise in their use to facilitate serious violent crime and drug trafficking.

As a result, the Commission commenced **Project Hakea** to investigate the use of tracking and other surveillance devices as an enabler of serious and organised crime in NSW.

An initial review of joint operations between the Commission and partner agencies identified frequent and increasing use of tracking devices to facilitate murders, public place shootings, kidnappings, violent drug thefts, and drug trafficking.

The Commission reviewed classified and open-source material, assessed existing legislative and regulatory frameworks, and deployed specialist capabilities and statutory powers to collect information that would be otherwise unavailable to law enforcement.

The Commission:

- collected and analysed sales of over 5,500 tracking devices to customers based in NSW since the beginning of 2023
- conducted eight coercive hearings to obtain evidence from witnesses in relation to the criminal use of tracking devices
- interviewed close associates of major OCNs to gain insights regarding the nature and scope of criminal use of tracking devices.

Chapters 1 and 2 of this report provide an overview of **Project Hakea** and outline the current legislative framework relating to tracking and other surveillance devices. Further contextual information is provided in **Chapters 8 and 9**.

Chapter 3 describes how tracking devices are part of the standard toolkit for violent organised criminals and sophisticated drug traffickers. The evidence indicates tracking devices are amongst the first items procured when planning an organised crime murder and OCNs consider them key for the success of each violent 'job'. Tracking devices are often transferred between criminals via clandestine exchanges in the same way as illicit drugs and firearms.

While the Commission set out to investigate the use of tracking devices by OCNs, our enquiries highlighted frequent use of tracking and other surveillance devices by domestic and family violence perpetrators. **Chapter 4** provides insight into the way that domestic violence perpetrators use tracking devices, often as part of a series of behaviours intended to intimidate, frighten, and control their intimate partners.

Disturbingly, the Commission found significant evidence of organised criminals using tracking devices to monitor, control, and test the "loyalty" of their intimate partners. The nexus between organised crime and domestic and family violence (DFV), which has long been observed by law enforcement practitioners, was undeniable in this investigation.

Chapter 5 presents an analysis of the sale of 5663 tracking devices, over an approximate 12 month period, since 1 January 2023. Through an extensive data matching process, the Commission identified and assessed 3147 customers, finding that:

- 37% of customers were adversely known to the NSW Police Force for relevant criminal behaviour (as defined in **Section 5.2**)
- 15% of customers were known to the NSW Police Force for involvement in serious and organised crime activity
- 25% of customers had a recorded history of domestic violence
- 126 customers were Apprehended Violence Order (AVO) defendants at the time they purchased a tracking device, including some customers who purchased a tracking device in the days after an AVO was enforced.

The Commission deemed 391 customers to be particularly high-risk and referred these matters individually to the NSW Police Force and other agencies. While our dataset was too large to investigate every customer with criminal history, the Commission conducted targeted intelligence probes that led to the discovery of three drug supply syndicates that were previously unknown to law enforcement.

Chapter 6 highlights a specific risk posed by some private investigators and specialist 'spy stores' who sell surveillance options to DFV perpetrators and other criminals. Our data analysis found that 40% of customers who purchased tracking devices from providers in this industry were known to the NSW Police Force for domestic violence or organised crime involvement. Some providers openly advertise the use of tracking and other surveillance devices for covert monitoring of intimate partners, and sell discreet surveillance devices along with other products, such as purported 'infidelity' test kits.

Tracking and other surveillance devices are unregulated items, in the sense that there is no requirement for retailers to be licensed, to collect accurate customer details, or to record device identifiers. The ramifications for law enforcement investigations and public safety are discussed in **Chapter 7**, including an example where a tracking device used to facilitate a public place shooting could not be traced back to a retailer or purchaser. This chapter also addresses limitations in the current legislation that make the investigation and prosecution of criminal use of tracking devices unduly difficult.

The **Findings** and **Recommendations** of this report call for actions that will encourage broad community awareness regarding criminal use of tracking devices, create a regulatory framework for the sale of tracking devices in NSW, and strengthen legislation to support law enforcement investigations and to increase accountability for offenders.

The recommendations also seek to reduce access to tracking devices by serious criminal offenders who are subject to AVOs, community-based sentences, and bail and parole conditions. Together, these recommendations seek to promote a safer NSW by making the operating environment more hostile to criminal offenders and networks.

Snapshot: NSW Tracker purchases reviewed

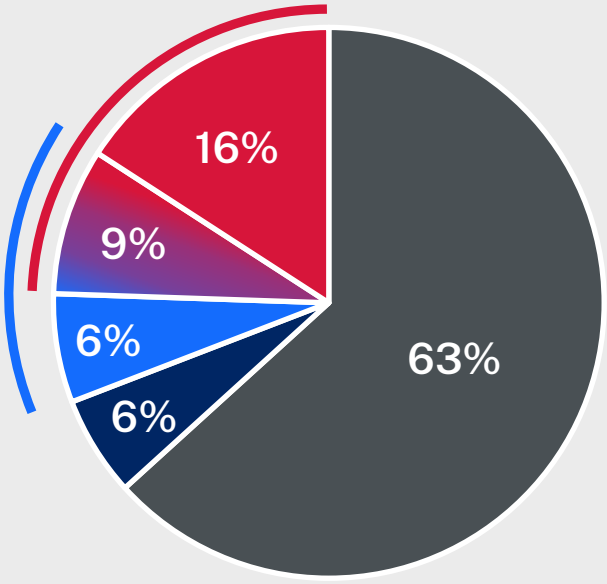
5663 trackers identified

4176 transactions reviewed

3147 customers assessed

Of assessed customers:

- **37%** were adversely known to police
- **25%** had a domestic and family violence background
- **15%** had a serious and organised crime background
- **6%** had a different criminal background
- **126** were AVO defendants at the time of purchase



391 high-risk customers referred to police

Intelligence reports or warnings established for all referrals

Some customers remain under investigation

The top 100 customers who purchased the most devices were:

2x more likely to be AVO defendants or charged with domestic and family violence

2.4x more likely to be known for serious and organised crime offending

Findings

1. Tracking and other surveillance devices are increasingly used to facilitate organised crime, including murder, kidnapping, and drug trafficking.

2. Tracking and other surveillance devices are frequently used by perpetrators of domestic and family violence (DFV) to stalk, harass, intimidate, and monitor victims, sometimes leading to violent outcomes. One in four known individuals who purchased tracking devices since the beginning of 2023 have a history of domestic violence.

3. There is a strong nexus between organised crime and DFV offending, with organised criminals using tracking devices to monitor and control their intimate partners.

4. Tracking and other surveillance devices are widely available in NSW and can be easily purchased from a range of local and overseas retailers, in person and online.

5. Some private investigators and 'spy stores' promote the illegal use of surveillance devices and offer illegal surveillance services to customers.

6. Charges laid under the *Surveillance Devices Act 2007* (NSW) significantly under-represent the true extent of offending involving tracking devices.

7. Law enforcement efforts to investigate criminal offences and locate tracking devices used by high-risk individuals are frustrated because:

    a. there are no licensing or registration requirements for suppliers of tracking devices, and suppliers do not have any due diligence, data collection, or mandatory reporting obligations;

    b. there are no licensing or registration requirements for purchasers or users of tracking devices in NSW; and

    c. identifiers of tracking devices (for example, the IMEI) are not required to be recorded prior to sale and suppliers do not record such data.

Recommendations

1. To reduce the malicious use of tracking devices, Government:
    a. work with industry to build in safety features, such as anti-stalking measures, on tracking devices; and
    b. restrict the sale and use of devices without such safety features. (See Section **4.5**).
2. In view of the evidence that criminals involved in serious organised crime and the perpetrators of domestic and family violence utilise tracking devices to commit offences, the Government reduce access to tracking and other surveillance devices by serious offenders through existing legislative frameworks, such as:
    a. directing Government legal representatives appearing before courts, tribunals, or similar authorities on Apprehended Violence Orders (AVOs), community-based sentences, and bail and parole applications, to make submissions in favour of the imposition of conditions restricting the purchase, possession, maintenance, and monitoring of tracking devices;
    b. amending the *Crimes (Domestic and Personal Violence) Act 2007* (NSW) to explicitly provide that AVOs may include a prohibition on the possession and use of tracking devices; and
    c. considering similar legislative amendments directed at offenders on community-based sentences, bail, and parole. (See Sections **5.4**, **5.6**, **7.4**).
3. Having regard to the finding that some private investigators and 'spy stores' promote the illegal use of surveillance devices and offer illegal surveillance services to customers, Government ensure that the legislative and regulatory changes in Recommendations 4 and 5 below are particularly applied to these industries. (See Chapter **6**).
4. Government regulate the sale of surveillance devices, including through:
    a. licensing for suppliers of surveillance devices;
    b. recording of device identifiers;
    c. recording of customer details;
    d. mandatory reporting of suspicious purchases. (See Section **7.2**).
5. Government strengthen legislation to:
    a. remove the requirement to obtain the Attorney General's consent to institute prosecutions under the *Surveillance Devices Act 2007* (NSW), beyond the amendment contained in the Bail and Other Legislation Amendment (Domestic Violence) Bill 2024 (NSW);
    b. prohibit the use of a surveillance device to facilitate serious criminal activity;
    c. prohibit the use of a surveillance device to facilitate a domestic violence-related offence;
    d. prohibit the monitoring of a surveillance device alongside the use, installation, and maintenance;
    e. prohibit the supply of a surveillance device with *recklessness* as to whether it will be used unlawfully, such as encouraging unlawful use of tracking devices in advertising material; and
    f. prohibit any activity that causes a surveillance device to be installed, used, or maintained without consent (including instructing another person to do so). (See Section **7.3**).

1 Introduction

1.1 About the Commission

The New South Wales Crime Commission (the Commission) is an independent law enforcement agency established under the *Crime Commission Act 2012* (NSW) (CC Act). The purpose of the Commission is to prevent, reduce, and disrupt organised and other serious crime in NSW. It does so through the powers and functions given to it under the CC Act, and through the confiscation of criminally derived proceeds under the *Criminal Assets Recovery Act 1990* (NSW).

The Commission conducts investigations into serious and organised crime (SOC). It also furnishes reports relating to organised and other crime and, where appropriate, makes recommendations for changes in the laws of the State.

1.2 Tracking devices in criminal offending

For two decades, the Commission has been aware of the criminal use of tracking devices within a SOC context. This use has escalated in recent years, particularly in organised crime violence since 2022.

In October 2023, the Commission commenced an examination into the use of tracking devices by reviewing its own investigation records and other law enforcement holdings. In March 2024, the Commission sought and obtained the *Hakea* reference from its Management Committee, to investigate the availability and criminal use of surveillance and counter-surveillance devices in NSW. The Commission received information and assistance from other law enforcement and government agencies, particularly the NSW Police Force, during the investigation.

The Commission applied many of the strategies used in typical criminal investigations, alongside significant data collection and analysis. This included using the Commission's powers under the CC Act and the *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA Act), analysis of law enforcement databases, and review of relevant academic and open-source material. Several matters relevant to our enquiries are subject of ongoing criminal investigations and cannot be discussed in this report.

This report focuses on the criminal use of tracking devices, reflecting the particularly significant use of tracking technology to facilitate the most serious types of criminal activity – homicide, drug trafficking, and other violent crime. Other surveillance devices such as optical and listening devices are also used for criminal purposes and are addressed to a lesser extent in this report.

1.3 Project Hakea objectives

The objectives of **Project Hakea** are to:

- collect information regarding the availability of surveillance devices in NSW;
- assess the nature and scale of criminal use of surveillance devices in NSW;
- disseminate intelligence to the NSW Police Force and other law enforcement agencies to inform a broader understanding of surveillance and devices, mitigate risk, and investigate and disrupt criminal activity enabled by surveillance devices; and
- identify vulnerabilities in current legislative, regulatory and policy frameworks, and opportunities for reform.

This report describes and analyses the criminal use of tracking and other surveillance devices in NSW and recommends changes to laws that will contribute to a safer community.

2 Definitions and legal framework

2.1 What is a tracking device?

The *Surveillance Devices Act 2007* (NSW) (SD Act) defines a tracking device as 'any electronic device capable of being used to determine or monitor the geographical location of a person or an object'. This encompasses a range of devices designed to track people, vehicles, personal items, and pets. This report primarily addresses Global Positioning System (GPS) tracking devices that are designed for monitoring the location of vehicles.

GPS tracking devices can be either battery-powered or hardwired. This report focuses on battery-powered devices, which are usually magnetic and can be covertly affixed to the undercarriage of vehicles. Magnetic battery-powered tracking devices are particularly appealing for criminal use, as they are easily concealed and do not require access to the inside of the vehicle to install. These devices range from the size of a coin up to a small box weighing between 200 and 450 grams.

GPS tracking devices require a Subscriber Identity Module (SIM) card to connect to the internet, and to send and receive text messages. As a result, they also have an International Mobile Equipment Identity (IMEI).[1] Some tracking devices also have a remote listening capability, which is activated by placing a phone call to the tracking device and listening to surrounding noise.

Location data from GPS tracking devices can be viewed in real-time on online monitoring platforms, which can be accessed via web portals and/or mobile applications. Most platforms also allow review of historical data, usually for a period of up to six months. Some tracking devices also provide locations via text message alerts.

Bluetooth tags (such as Apple AirTags, Samsung Smart Tags, and Tiles) are commonly used to track personal items such as wallets, keys, and luggage. Bluetooth tags are also used for criminal purposes and are noted in this report.

Background information regarding the availability and genuine uses of tracking devices is provided in **Chapter 9**.

GPS tracking devices	Bluetooth tags and tiles
Purpose: Monitoring the location of vehicles, as well as other personal items.	**Purpose:** Loss prevention for personal items such as keys, wallets, bags, and luggage.
Size: Coin-sized to a small box.	**Size:** Small and easily fitted to keychains.
Technology: Location data is derived from Global Navigation Satellite System technology.	**Technology:** Location data is derived from Bluetooth technology, which relies on a mesh network of nearby Bluetooth devices.
Battery: Rechargeable battery that generally lasts up to several weeks without charge.	**Battery:** Battery life can range between 1 and 3 years, with some brands offering replacement batteries.
Identifiers: Serial number and IMEI.	**Identifiers:** A serial number can often be located under the battery.

[1] An IMEI is a unique 15 or 16 digit number which is used to identify devices connected to a mobile network.

GPS tracking devices	Bluetooth tags and tiles
Features: Online or app-based monitoring platforms can be accessed by anyone with login credentials.	**Features:** App-based monitoring, which sometimes can be accessed by more than one person.
Anti-Stalking: No in-built anti-stalking mechanisms.	**Anti-Stalking:** Tags and tiles generally have anti-stalking mechanisms, including 'unknown tracker' alerts.
Installation features: Magnetic or hardwired options available.	**Installation features:** No in-built feature for attaching to items. However, they can be placed inside small magnetic boxes.

2.2 Legal framework

The SD Act regulates the installation, use, maintenance, and retrieval of surveillance devices in NSW. It provides law enforcement with a framework for the use of surveillance devices in criminal investigations and prosecutions, while protecting against unnecessary intrusion into the privacy of individuals. While this report focuses on tracking devices, the SD Act also applies to listening devices, optical devices, and data surveillance devices (see definitions provided in **Appendix B**).

A general prohibition against the installation, use, and maintenance of tracking devices without consent is provided in section 9 of the SD Act. There are similar prohibitions relating to the use of optical, listening and data surveillance devices without consent. The SD Act also prohibits the manufacture, supply and possession of a surveillance device with the intention for the device to be used in contravention of the SD Act. All of these offences carry a maximum penalty of five years imprisonment.

NSW Police Force records show that between 2010 and 2023, 96 individuals were charged with unlawful use of a tracking device under section 9 of the SD Act, of which 90 were male. On 79 occasions the offence was domestic violence-related, on 14 occasions the offence was organised crime-related, and the remaining instances did not fall in either category.

Limitations within the legislative and regulatory framework for surveillance devices are discussed in **Chapter 7**, and an analysis of charges laid under the SD Act is provided in **Chapter 8**.

Law enforcement agencies lawfully deploy tracking and other surveillance devices pursuant to warrants issued under the SD Act and the *Surveillance Devices Act 2004* (Cth). The findings and recommendations of this report are not intended to report on, or impact the lawful use of surveillance devices by law enforcement.

3 Use of tracking devices in serious organised crime

Organised and other serious offenders widely and increasingly use commercially available tracking technology to facilitate their crimes. Violent criminals deploy tracking devices to plan acts of targeted violence, including murders, kidnappings, public place shootings, and home invasions. Organised crime networks (OCNs) use tracking devices to facilitate the importation of illicit drugs and manage onshore drug distribution.

The analysis in this section is supported by evidence given during eight coercive examinations of individuals who are members of, or directly associated with, OCNs in NSW. To protect the safety of the witnesses, this section does not relay specific details from their evidence. The Commission also conducted interviews with several close associates of OCNs to inform the investigation.

3.1 Organised crime violence

The investigation established that tracking devices have featured in at least 20 completed or attempted acts of organised crime violence, including three murders, three planned or attempted murders, one drive-by shooting, three kidnappings, five planned or attempted kidnappings, one home invasion, and four planned or attempted violent drug thefts since 2016. Fifteen of these 20 events occurred since 2022, reflecting the increasing prevalence of tracking in organised crime violence.

OCNs generally deploy tracking devices on a target's vehicle days or weeks prior to the planned violent crime to identify their place of residence and monitor their movements. They use location data from tracking devices to devise a plan for where, when, and how to carry out the actual offence. Occasionally, organised crime figures discover tracking devices on their vehicles prior to a planned offence, which can lead to dangerous pre-emptive action.

Case Study 1

In 2023, the discovery of a tracking device allegedly caused a senior organised crime figure to order a shooting that mistakenly targeted three innocent members of the public. The organised crime figure discovered a tracking device that had been covertly affixed to his vehicle, leading him to suspect that a rival OCN was planning to murder him. The crime figure recruited a crew to provide protection of his residence. A member of the crew opened fire on two suspicious vehicles, which were in fact occupied by innocent members of the public. The alleged shooter killed one person and injured another two.

Over the past year, the Commission has identified specific OCNs that have deployed tracking devices in preparation for acts of violence. For example, an OCN reportedly deployed tracking and other surveillance devices against a rival in early 2024 in preparation for a murder that was either aborted or has not yet eventuated. This information was provided to relevant law enforcement and intelligence agencies.

> In an interview with a criminal associate of an OCN, the Commission was told that OCNs involved in organised violence consider tracking devices to be key for the success of each 'job'.

Case Study 2

Tracking devices were used to plan the murder of Alen Moradian in 2023. Moradian was a high-profile organised crime figure who was shot and killed as he entered his vehicle in the underground carpark of his apartment building. Prior to the murder, a tracking device was placed on the vehicle of Moradian's wife while she was visiting a family member. The OCN monitored the movements of the tracking device to identify the location of Moradian's residence when his wife returned home. The following evening, two alleged offenders tasked with conducting surveillance of Moradian's residence installed a second tracking device on the same vehicle. The murder was carried out two days later.

The NSW Police Force investigation identified that the accounts for the online platform used to monitor the tracking devices were created using fictitious details. Similarly, the mobile phones used to access the online monitoring platform were fitted with SIM cards registered in false names. The devices themselves were purchased by an associate of the primary offenders.

Tracking devices have enabled the emergence of 'contract crews', hired to carry out serious acts of violence. 'Contract crews' are specialised criminal groups who negotiate contracts with major OCNs to undertake acts of violence, including murder, kidnapping, and drug theft. The Commission is aware of at least three major OCNs in Sydney that employ 'contract crews' of this nature.

Tracking devices are usually the first items purchased and deployed when contract crews accept a 'job'. Alongside tracking devices, 'contract crews' use a range of surveillance techniques, including physical surveillance, online research, and drones. The Commission is aware that OCNs involved in organised violence consider tracking devices to be key for the success of each job.

Case Study 3

A 'contract crew' operating on behalf of a Sydney-based organised crime figure carried out at least two kidnappings during 2023 and were arrested while planning a third. While detained, the crew subjected their victims to violent assaults to induce ransom payments from family and friends.

Members of the crew deployed tracking devices on the vehicles of prospective kidnapping victims to monitor their movements and frequent locations. They also used the devices to identify the optimal time to carry out the kidnappings. The crew removed the devices during the kidnappings in an attempt to avoid them being discovered by law enforcement.

3.2 Drug importation, supply, and theft

GPS tracking devices and Bluetooth tags are used by OCNs to facilitate the importation and distribution of illicit drugs. OCNs commonly embed tracking devices within illicit drug packages and install devices on the vehicles used by drug 'couriers' employed to distribute illicit drugs. They review the location data of tracking devices to coordinate drug deliveries to customers and to monitor couriers to ensure they are not stealing the drugs. Tracking devices can also alert criminals to intervention by law enforcement or rival OCNs.

Tracking devices are sometimes embedded in illicit drug consignments to allow overseas and onshore arms of the OCN to monitor the movement of consignments while enroute to Australia. Tracking devices are also used to retrieve illicit drug importations from secure locations, such as ports, container yards, and freight forwarders. Retrievals are often outsourced to specialised crime groups who break into these locations and use tracking data to pinpoint the exact location of the drug consignment.

It is common for OCNs to steal illicit drugs from rivals and such theft generally requires an OCN to uncover the locations used by rivals to store their illicit drugs. The Commission is aware of numerous instances where tracking devices have been installed on the vehicles of rival drug couriers to identify the rival OCN's storage location.

Case Study 4

In 2023, a specialist OCN attempted to retrieve a large commercial quantity of illicit drugs from a shipping container. The OCN was provided with the details of the shipping container. The intention of the OCN was to intercept the container and retrieve the illicit drugs. Enquiries identified that a tracking device was placed in the shipping container after it arrived in NSW. The OCN monitored the movements of the tracking device to identify a suitable opportunity to break into the container and retrieve the drugs. The OCN gained unlawful access to a location to examine the container, but failed to retrieve the drugs.

3.3 Device acquisition and handling

OCNs adopt measures to create distance between themselves and tracking devices used for criminal purposes. Criminals often purchase tracking devices using fictitious identification details or recruit third parties to purchase devices on their behalf.

Despite tracking devices not being prohibited equipment, criminal networks sometimes transfer tracking devices via covert exchange or dead drop – a procedure where an item is left in a pre-arranged location for the recipient to retrieve. These exchange techniques are commonly used to convey prohibited items such as illicit drugs or weapons.

Falsely subscribed SIM cards are often installed in tracking devices used for organised crime activity. OCNs can easily obtain SIM cards subscribed in fictitious or fraudulently obtained details, and these are commonly installed in mobile phones or tracking devices used for criminal purposes.

The Commission reviewed a sample of 17 tracking devices that were used in organised crime violence or seized by the NSW Police Force from organised crime figures, and found that none of these devices had SIM cards subscribed in the name of the primary owner. Most of the SIM cards were registered in false or fictitious details.

Case Study 5

An investigation conducted by the NSW Police Force identified an offender who was involved in purchasing and installing tracking devices on behalf of a Sydney-based OCN.

Tracking devices set up by the offender were installed on the vehicles of several individuals in 2023. The deployment of these tracking devices facilitated serious violence offences, including a home invasion and a public place shooting. At least some of the devices were purchased by the alleged offender under a fictitious name and were paid for in cash. The alleged offender installed falsely subscribed SIM cards into the tracking devices and monitored the location data using a mobile phone that was also registered in false details.

In 2023, the NSW Police Force charged the alleged offender with four offences relating to the unlawful use of tracking devices. The matter remains before the courts.

Finding 1

Tracking and other surveillance devices are increasingly used to facilitate organised crime, including murder, kidnapping, and drug trafficking.

4 Use of tracking devices in domestic and family violence

While the Commission initially sought to investigate the use of tracking devices by OCNs, our enquiries highlighted frequent use of tracking devices by domestic and family violence (DFV) perpetrators to stalk, intimidate, monitor, and harass victims. Location tracking is often used as part of a series of malicious behaviours which seek to control an individual within a relationship. These behaviours pose a significant risk to the physical safety and mental health of DFV victims.

4.1 Prevalence of tracking devices in DFV offending

In 2020, the Second National Survey of Technology Abuse and Domestic Violence in Australia by the Women's Services Network (WESNET) reported an increased uptake of accessible digital technologies by DFV perpetrators to control and monitor victims.[2] The report, which was based on a nation-wide survey of frontline DFV practitioners, identified a 245% increase between 2015 and 2020 in DFV victims being tracked with GPS apps or devices.

The Commission found evidence of frequent use of tracking devices by DFV perpetrators. As discussed in **Chapter 2**, the Commission found that of the 96 offenders charged with unlawful use of tracking devices between 2010 and 2023, 79 were charged in relation to a domestic violence event. This represented 82% of offenders. Furthermore, as detailed in **Chapter 5**, the Commission identified that nearly 25% of known individuals who purchased tracking devices since 2023 have a history of domestic violence.

There is a significant body of evidence that the most dangerous period for DFV victims is the period immediately following a separation, with 58% of intimate partner homicides occurring after a planned or actual separation.[3,4] The Commission found that 75% of offenders charged with DFV-related tracking device offences under the SD Act started tracking the victim following a separation. For nearly two-thirds of offenders in this subset, the tracking commenced within a 3-month period after separation.

The Commission is also aware of two offenders who continued to monitor their partners while incarcerated for domestic violence offences. This included monitoring the location of undetected trackers using illegal phones and requesting third parties to contact and follow their partners. Both were charged for this subsequent offending.

> 82% of offenders charged by the NSW Police Force with unlawfully using a tracking device were committing domestic violence offences.

[2] Woodlock, D., Bentley, K., Schulze, D., Mahoney, N., Chung, D., and Pracilio, A., (2020). Second National Survey of Technology Abuse and Domestic Violence in Australia. WESNET.

[3] A planned separation can include circumstances where a victim has informed the offender they are leaving or taken steps to leave the relationship, such as looking for alternative accommodation or gathering items required to leave an abuser.

[4] Family, domestic and sexual violence: Domestic homicide: https://www.aihw.gov.au/family-domestic-and-sexual-violence/responses-and-outcomes/domestic-homicide#separation, last accessed 17 June 2024.

4.2 Stalking and intimidation

DFV perpetrators maliciously use tracking devices to gain information about the victim's whereabouts for the purpose of intimidating, stalking, or humiliating them – with many perpetrators making the victim aware that they are being tracked. The Commission also reviewed cases where DFV perpetrators used location data from tracking devices to threaten or carry out violence against their partner or their partner's family.

The Commission reviewed more than a dozen NSW Police Force investigations that were initiated after the offender directly told the victim they had placed a tracking device on their vehicle. All of these offenders were male. The offender often informed the victim that they were using a tracking device to gather information about the victim's new address or new partner, or that they intended to use the location data to defame the victim in Court or within their social circles. In other cases, the victim discovered a tracking device themselves after growing suspicious that the offender appeared to constantly 'bump into' them in public spaces.

Data collected by the Commission shows that DFV offenders demonstrated ongoing and persistent stalking behaviours which were facilitated by tracking devices. DFV offenders often purchased multiple devices to track the same victim, and many offenders charged under the SD Act were in possession of numerous tracking devices at the time of their arrest.

Offenders also engaged in other stalking behaviours, such as physical surveillance, monitoring location-based mobile phone applications, and using other types of surveillance devices to monitor their victims. In some circumstances, offenders deployed tracking devices after alternative forms of monitoring were cut off, for example, when phone applications were disabled by victims.

Case Study 6

An investigation by the NSW Police Force identified a male with a recorded history of DFV offending including using surveillance devices to monitor his former partner. NSW Police Force enquiries established that the offender had purchased more than 15 devices from an online marketplace. NSW Police Force officers found both a magnetic and a hardwired GPS tracking device installed in the victim's vehicle. The victim reported three other events during which she discovered devices on her vehicle and inside her home. The offender was convicted for stalking, illegally using surveillance devices, and contravening an AVO. He received a Community Correction Order with no custodial sentence.

4.3 Coercive control

On 1 July 2024, new laws criminalising coercive control will come into effect in NSW. The *Crimes Legislation Amendment (Coercive Control) Act 2022* (NSW) will amend the *Crimes Act 1900* (NSW) to criminalise abusive behaviour directed towards current or former intimate partners. The definition of abusive behaviour will include 'behaviour that *[...]* monitors or tracks a person's activities, communications or movements, whether by physically following the person, using technology or in another way'.[5]

[5] Section 54F(2)(e), *Crimes Act 1900* (NSW)

The use of tracking devices can play a key role in an offender's controlling behaviour. The Commission identified individuals who were charged for the use of a tracking device but who also clearly met the definition for other abusive behaviours defined under the coercive control legislation. In these instances, the offender often used the tracking device to control the victim's movements and harass them during their day-to-day activities. Under the forthcoming laws, the use of tracking devices can form evidence of a coercive control offence.

Case Study 7

The victim and offender had been in a long-term relationship before separating. During the relationship, the offender had forced the victim to share her location via a mobile phone application. The offender also engaged in other controlling behaviours, including threatening to distribute intimate photos of the victim. After separating, the offender sent messages to the victim indicating he was tracking her location using GPS trackers attached to her own vehicle and a vehicle used by a family member. The offender was charged under the SD Act. This charge was later withdrawn, but the offender was convicted for related offences and received both a Community Correction Order and an Intensive Correction Order.

The use of tracking devices may indicate a significant risk of future violence, including lethal violence against a DFV victim. Research conducted by Australia's National Research Organisation for Women's Safety (ANROWS) indicates that 33% of offenders who committed intimate partner homicides were 'fixated' on their current or former partners.[6] These offenders were likely to exhibit controlling behaviours, and to monitor the victim including through location tracking. A separate meta-analysis also reported that stalking behaviour increased the likelihood of intimate partner homicide by 2.79 times.[7] The Commission is aware of domestic violence homicides in which tracking devices were used as early as 2008. The NSW Domestic Violence Death Review Team provided the following case study from 2016.

Case Study 8

A male offender shot and killed his wife in regional NSW before shooting himself. The couple had been married for more than 25 years and were not known to law enforcement for any previous domestic violence. Their relationship had been deteriorating for about four months before the homicide and the victim had expressed a desire to leave the relationship. In the month before the murder, the offender had used a GPS tracking device, purchased from an instore automotive parts retailer, to monitor the victim's movements. This tracking occurred until at least the day before the murder, and the offender's children and neighbour were aware the tracking was occurring. The tracking appeared to form part of a series of behaviours that the offender used to prevent the victim from leaving the relationship.

[6] Boxall, H., Doherty, L., Lawler, S., Franks, C., & Bricknell, S. (2022). The "Pathways to intimate partner homicide" project: Key stages and events in male-perpetrated intimate partner homicide in Australia (Research report, 04/2022). ANROWS.

[7] Spencer, C & Stith, S. (2020) Risk Factors for Male Perpetration and Female Victimization of Intimate Partner Homicide: A Meta-Analysis. Trauma, Violence, & Abuse.

4.4 Under-reporting of tracking in DFV offending

The use of tracking devices in DFV offending is grossly under-reported and under-prosecuted. As documented throughout this report, the number of charges laid under the SD Act in relation to tracking is low. Beyond the findings of this report, publicly available reporting also indicates that tracking devices are frequently detected on the vehicles or other belongings of DFV victims. For example, a security group recently stated that they find up to six 'tile' devices each week on vehicles across Australia.[8]

This is consistent with the general under-reporting of both DFV offending and technology-facilitated abuse. An ANROWS study published in 2022 found that one in three individuals who experienced technology-facilitated abuse did not tell anyone about their experience, and more than 90% did not report their experience to police.[9] Low rates of reporting of DFV were further noted during COVID-19 lockdowns,[10] and DFV peak bodies consistently find significant under-reporting of DFV.[11]

Finding 2

Tracking and other surveillance devices are frequently used by perpetrators of domestic and family violence (DFV) to stalk, harass, intimidate, and monitor victims, sometimes leading to violent outcomes. As identified below in **Section 5.6**, one in four known individuals who purchased tracking devices since the beginning of 2023 have a history of domestic violence.

4.5 Safety features of tracking devices

Malicious tracking is often covert by nature and intended to be undetected by victims. Tracking devices can be placed in inconspicuous areas where they are unlikely to be discovered, including the undercarriage of vehicles. GPS tracking devices are not equipped with safety or anti-stalking mechanisms, meaning that there is no easy method to detect GPS tracking devices other than physical inspection.

Bluetooth tags and tiles sometimes have anti-stalking mechanisms that alert people who are moving in tandem with the device. While some anti-stalking systems are effective, their reliability and functionality vary significantly across brands. Most notably, Apple AirTags have two safeguards when they are detected to be travelling with an un-paired device: a notification system that sends an alert to the un-paired device, and a beeping sound emitted by the AirTag. The alert contains basic information about the AirTag, including its serial number and the last four digits of the phone number of the person who registered the device.

In May 2024, Apple and Google jointly announced the roll out of a capability that allows users across iOS (Apple) and Android (Google) to be alerted if an unknown Bluetooth device is moving with them

[8] https://7news.com.au/news/disturbing-ways-technology-is-used-to-control-and-track-domestic-violence-victims-c-14935486, last accessed 17 June 2024.

[9] Powell, A., Flynn, A., Hindes, S. (2022). Technology-facilitated abuse: National survey of Australian adults' experiences, ANROWS.

[10] Carrington, K., Morely, C. Warren, S., Ryan, V., Ball, M., Clarke, J., Vitis, L. (2021). The impact of COVID-19 pandemic on Australian domestic and family violence services and their clients. Australian Journal of Social Issues.

[11] See for example: https://www.dvnsw.org.au/resources/domestic-family-violence-statistics, last accessed 17 June 2024.

over time.[12] This cross-platform capability has been implemented in iOS 17.5 and Android 6.0+ devices. For users to be alerted, Bluetooth tags must be compatible with an industry specification, called 'Detecting Unwanted Location Trackers', which Apple and Google have publicly released. Separately, there are a range of existing mobile phone applications available to both iOS and Android users, which allow users to scan their surroundings for Bluetooth devices.

Case Study 9

In late 2023, a male offender was reported to be engaged in stalking behaviour aimed towards a female victim, who was his former partner. The victim reported seeing the offender drive past her house multiple times per day and received dozens of phone calls seemingly from the offender.

When the victim became suspicious that she was being physically tracked by the offender, she utilised used an anti-stalking mobile phone application to find an Apple AirTag affixed to her vehicle inside a magnetic box. The offender was charged and received a 12-month Community Correction Order.

Recommendation 1

To reduce the malicious use of tracking devices, Government:

a. work with industry to build in safety features, such as anti-stalking measures, on tracking devices; and

b. restrict the sale and use of devices without such safety features.

4.6 Nexus between organised crime and DFV offending

This investigation identified a strong nexus between organised crime and DFV offending involving tracking devices. The Commission found that one-third of offenders charged under the SD Act with unlawfully using tracking devices were also associated with OCNs. The majority of these SOC offenders were charged with deploying trackers as part of DFV offending, rather than for organised crime activity.

The Australian Institute of Criminology reported that 40% of Outlaw Motorcycle Gang (OMCG) members have been charged with a domestic violence offence.[13] OMCG members were also twice as likely to have been charged with domestic violence offences than the general male offending population. In joint operations undertaken by the Commission, it is not unusual for investigators to incidentally uncover serious DFV offending perpetrated by organised crime figures.

Domestic violence perpetrators involved in SOC activity often use their criminal skillset against their current and former partners. For example, an organised crime figure with a history of involvement in armed robbery and prohibited drug supply allegedly used various surveillance devices against his

[12] https://www.apple.com/au/newsroom/2024/05/apple-and-google-deliver-support-for-unwanted-tracking-alerts-in-ios-and-android/, last accessed 17 June 2024.

[13] Morgan, A., Cubitt, T., and Dowling, C. (2023), Outlaw motorcycle gangs and domestic violence, Trends & issues in crime and criminal justice.

intimate partner. Furthermore, information received by the Commission indicates it is common for organised crime figures to track their partners as a means of testing their "loyalty". Victims may be fearful to report this abuse, as they may be perceived to be providing information to law enforcement about the offender's other criminal activity.

Case Study 10

A NSW Police Force investigation into the suspected drug supply activities of two male offenders identified the offenders using a tracking device to monitor the movements of one of the offender's ex-partner. The female victim approached the NSW Police Force to report incidents of her being stalked, tracked, and harassed. NSW Police Force officers examined her vehicle and located a magnetic GPS tracking device hidden underneath it. Both offenders were charged under the SD Act.

At the time of offending, both offenders were subject to parole conditions relating to previous drug supply offences, and one of the offenders was the defendant on an Apprehended Domestic Violence Order (ADVO) protecting the victim of this offence.

Finding 3

There is a strong nexus between organised crime and DFV offending, with organised criminals using tracking devices to monitor and control their intimate partners.

5 Tracking devices sold in NSW since 2023

Tracking devices are widely available for purchase from local and international retailers, including online marketplaces, electronics stores, automotive parts stores, specialty 'spy stores',[14] and private investigators. There is no readily available, reliable data indicating how many devices are sold each year.

The Commission served a sample of 20 retailers with notices issued under section 29 of the *Crime Commission Act 2012* (NSW), that required the production of data relating to the sale of tracking devices to NSW customers since 1 January 2023.[15]

The Commission received data for 4176 transactions. A total of 5663 tracking devices were sold across these transactions, including 4287 magnetic tracking devices, 1222 hardwired tracking devices, and 154 devices that could not be categorised due to unclear product descriptions.[16] The Commission did not review data relating to the sale of Bluetooth tags and tiles. Further information regarding this dataset is provided in **Appendix A**.

This section contains analysis of sales and customer data associated with these 4176 transactions.

4176 transactions

5663 trackers

3147 customers assessed

20 retailers

4287 magnetic

1222 hardwired

391 police referrals

Finding 4

Tracking and other surveillance devices are widely available in NSW and can be easily purchased from a range of local and overseas retailers, in person and online.

5.1 Missing and false details provided by customers

In 194 transactions, the customer provided either no name (88 transactions), a partial name (28 transactions), or a false name (78 transactions). Some customers provided their name as a random phrase or string of letters. One customer who was based in Queensland, and therefore not included in this dataset, falsely provided their name as 'Bill Cosby'.

[14] 'Spy stores' are businesses that sell gadgets and software used for covertly monitoring other people.

[15] Most retailers provided data from 1 January 2023 to 31 December 2023, although some retailers also provided data from the first quarter of 2024.

[16] The number of magnetic tracking devices exceeded the number of hardwired devices because the Commission prioritised approaches to entities known to sell magnetic devices.

5.2 Tracking devices purchased by people with criminal involvement

Within the dataset, the Commission identified 3248 unique customers who purchased either magnetic or hardwired tracking devices. Of these customers, 3147 were recorded in the NSW Police Force's Computerised Operational Policing System (COPS) database.[17] The Commission reviewed data for each of these 3147 customers dating back to 2010.[18]

The Commission identified 1156 customers who had relevant adverse history on the COPS database, representing 37% of the customers reviewed. For the purpose of this analysis, the Commission defined 'relevant adverse history' as any customer with at least one criminal charge, at least one record of being the person of interest in a domestic violence event, or at least one intelligence report relating to SOC activity. Individuals with adverse histories included serious domestic violence offenders, drug traffickers, violent criminals, and many who were a combination of these. The remaining 1991 customers did not have a criminal history, and may have been known to the NSW Police Force only as a witness or victim of crime.

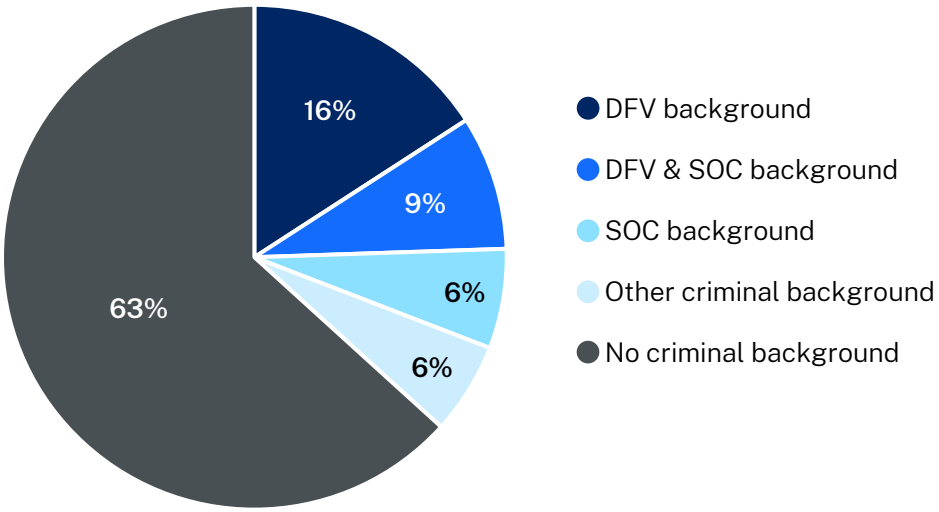


Figure 1: Criminal involvement of customers purchasing tracking devices

> 37% of customers who purchased tracking devices were adversely known to the NSW Police Force.

Only two of the 3147 customers reviewed had been charged with offences under the SD Act – both in 2024. One customer was charged with unlawful use of a tracking device, and the other customer was charged in relation to the use of a listening device that also contained GPS tracking capabilities. Both SD Act charges have since been withdrawn, but both offenders were also charged with domestic violence offences in relation to these events.

[17] COPS is an operational database which is used by the NSW Police Force to record information about offenders, victims, arrests, and events and intelligence reports.

[18] COPS database information prior to 2010 was not analysed due to data access limitations. The data in this section is accurate as at 28 May 2024.

5.3 Referral of high-risk customers

The Commission referred 391 customers, assessed as being 'high-risk', to the NSW Police Force and other relevant law enforcement and intelligence agencies. The Commission undertook a continuous triage and referral process to mitigate safety risks to potential victims. In almost all cases, the fact that these individuals had purchased tracking devices was not previously known to the NSW Police Force.

The Commission assessed customers based on their involvement in serious or recent DFV offending or reported links to SOC activity. Many customers referred were defendants on enforceable ADVOs. Of the 391 customers the Commission referred, 160 were known to the NSW Police Force in relation to DFV offending, 42 were known for SOC involvement, and a further 189 were known for both DFV and SOC offending.

Some of the individuals the Commission referred were already under NSW Police Force investigation or came under investigation following the Commission's referral. Where requested, the Commission assisted investigating officers by providing additional information about the customer's purchases.

5.4 General criminal history

Of the 3147 customers reviewed, 747 (approximately 24%) had been charged on one or more occasion since 2010. A total of 204 customers had been charged on five or more occasions, and 103 had been charged on ten or more occasions.[19]

Of the 747 customers with criminal history, 443 customers had been charged with at least one serious indictable offence.[20] There were also 39 customers charged with at least one offence carrying a penalty of 25 years imprisonment or more, and 16 charged with at least one offence carrying a penalty of life imprisonment, and 31 charged with at least one serious personal violence offence.[21]

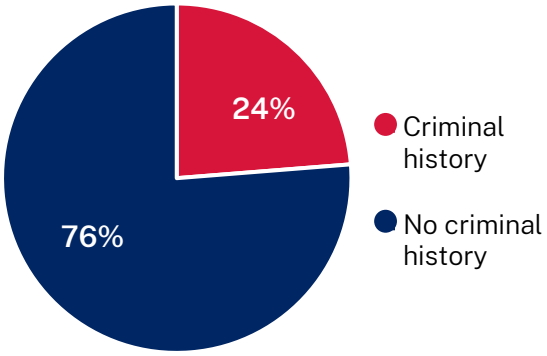


Figure 2: Criminal history of customers purchasing tracking devices

5.5 Serious and organised crime offenders

Of the 3147 customers reviewed, 472 (15%) were recorded in the COPS database in relation to SOC activity.[22] This includes several current and previous targets of joint investigations undertaken by the Commission and partner agencies into high-level OCNs.

[19] These figures refer to the total number of charge reference numbers or 'H numbers'. See Appendix B for further explanation.

[20] Section 4 of the *Crimes Act 1900* (NSW) defines a 'serious indictable offence' as an indictable offence that is punishable by imprisonment for life or a term of five years or more. 326 of these 443 customers had at least one serious indictable offence proven in court.

[21] The Commission has followed the definition of Serious Personal Violence Offence (SPVO) provided in subsection 16B(3) of the *Bail Act 2013* (NSW).

[22] This calculation was based on intelligence reports in the COPS database that had an 'associated factor' relating to SOC activity.

> 15% of the people who purchased tracking devices in NSW since 2023 were known to the NSW Police Force for their involvement in serious and organised crime.

Ninety-eight customers had been charged with at least one serious drug trafficking offence.[23] Of these customers, 64 had at least one serious drug trafficking offence proven in court.

Sixty-six customers had been subject to NSW Police Force action relating to firearms activity. Forty-one customers had at least one firearms-related charge, of which 19 had also been subject to a Firearms Prohibition Order (FPO). A further 25 customers had been subject to an FPO, although had not been charged with related offences.

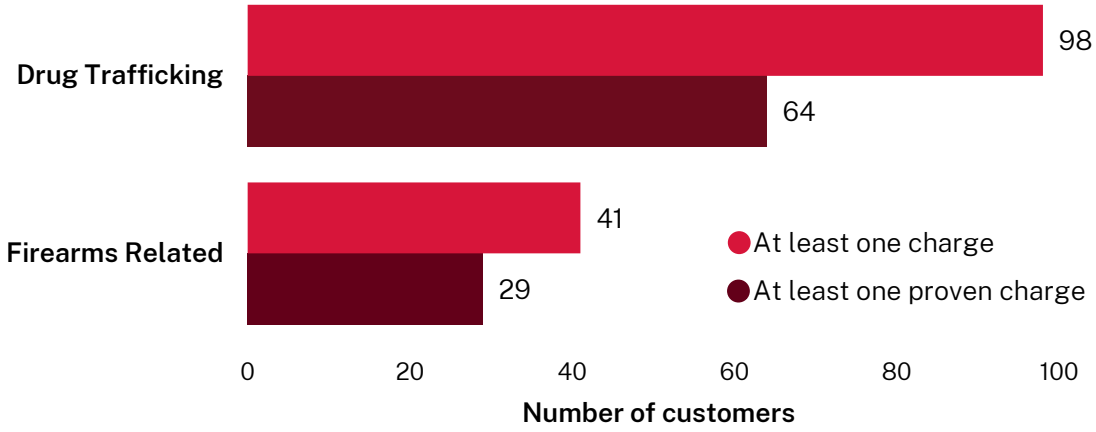


Figure 3: Customers with serious crime charges

The Commission also conducted intelligence probes into a small number of customers linked to OCNs, which resulted in the discovery of three drug supply syndicates that were previously unknown to law enforcement. These matters are ongoing.

5.6 Domestic and family violence offenders

Domestic and family violence offenders constituted the largest criminal cohort within the Commission's list of customers. Many customers the Commission referred to the NSW Police Force had previously used GPS tracking devices, AirTags, or other means to stalk their current or former intimate partners. Others were subject to reports by current or former partners who believed they were being monitored, but whose concerns were unproven.

The criminal history of DFV offenders who purchased devices was often extensive. The Commission's review of these individuals regularly revealed DFV history spanning decades, including against multiple partners or other relatives. Many had recent charges for domestic violence assault, contravention of AVOs, and sexual violence.

[23] The Commission has followed the definition of a drug trafficking offence provided in subsection 6(2) of the *Criminal Assets Recovery Act 1990* (NSW).

Almost 25% of customers were adversely known to the NSW Police Force for domestic violence.

A total of 770 identified customers had been recorded as the person of interest in at least one domestic violence event, representing almost 25% of all customers.[24] Of these 770 customers, 169 had been recorded as the person of interest in five or more domestic violence events, and 80 had been recorded in ten or more events.

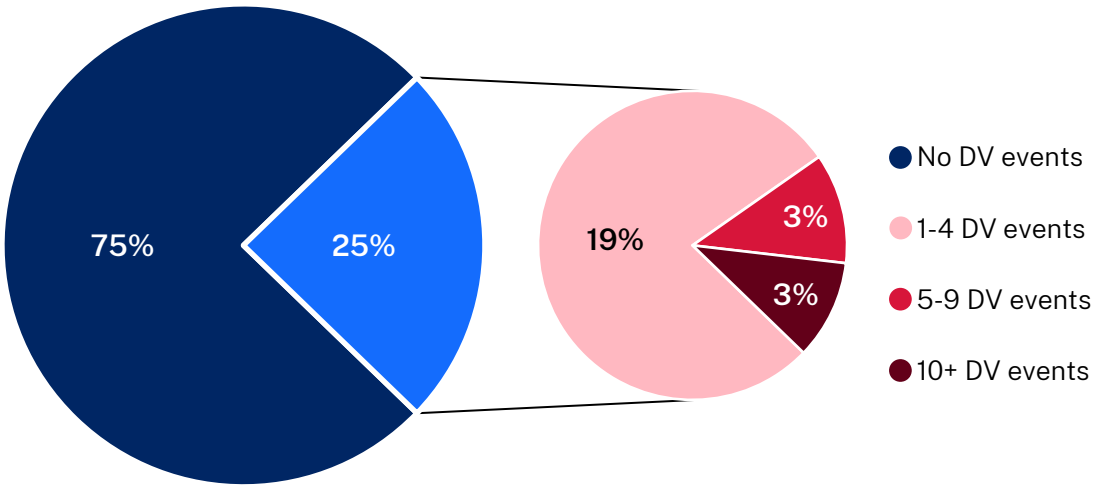


Figure 4: Customers recorded as persons of interest in domestic violence events

A total of 291 customers had been charged with at least one domestic violence-related offence, representing 9% of all customers.[25] Of these, 17 had five or more domestic violence-related charges proven in court.

Of the 3147 customers reviewed, 126 were the defendant (person named) on an AVO at the time they purchased a tracking device.[26] This included customers who purchased tracking devices in the days after they became subject to an AVO that prohibited direct contact with the victim. A further 90 customers became defendants on AVOs at some point after they purchased a tracking device. Together, these 216 customers represent 7% of all customers reviewed.

126 customers were the defendant on an AVO at the time they purchased a tracking device.

[24] The Commission defined a domestic violence event based on the incident category or associated factor assigned to the event. The person of interest (POI) in a domestic violence event is generally determined by the police officer/s who attend the scene or take the report.

[25] The Commission has followed the definition of a 'domestic violence offence' provided in section 11 of the *Crimes (Domestic and Personal Violence) Act 2007* (NSW).

[26] An 'AVO' can refer to either an ADVO, or an Apprehended Personal Violence Order (APVO); the type of which is generally not specified in this analysis. However, the vast majority of the data represents ADVOs.

The Commission identified 110 customers who had been charged at some point with contravening an AVO.[27] There were 46 customers who had been charged on three or more occasions with contravening an AVO, and 20 who had been charged on five or more occasions. In one instance, a tracking device was sold to a customer who had been charged on 13 occasions with contravening an AVO.

Recommendation 2

In view of the evidence that criminals involved in serious organised crime and the perpetrators of domestic and family violence utilise tracking devices to commit offences, the Government reduce access to tracking and other surveillance devices by serious offenders through existing legislative frameworks, such as:

a. directing Government legal representatives appearing before courts, tribunals, or similar authorities on Apprehended Violence Orders (AVOs), community-based sentences, and bail and parole applications, to make submissions in favour of the imposition of conditions restricting the purchase, possession, maintenance, and monitoring of tracking devices;

b. amending the *Crimes (Domestic and Personal Violence) Act 2007* (NSW) to explicitly provide that AVOs may include a prohibition on the possession and use of tracking devices; and

c. considering similar legislative amendments directed at offenders on community-based sentences, bail, and parole.

Further information relating to conditions on AVOs and other orders, and opportunities to reduce criminal use of tracking devices, is outlined in **Section 7.4**.

5.7 Frequent and suspicious customers

The Commission identified many customers who purchased tracking devices on multiple occasions. Some datasets also contained records of customers purchasing suspicious combinations of surveillance equipment, counter-surveillance devices, weapons, spyware, and privacy software.

The Commission applied triaging methods to identify customers exhibiting these behaviours and completed referrals to the NSW Police Force where necessary. The following table lists examples of suspicious individuals who purchased a high volume of tracking devices.

[27] All 110 customers had been charged with contravening an ADVO, while 35% also had charges for contravening an APVO.

Customer	Number of devices purchased since 2023	Criminal history
Customer 3075	11 (All magnetic)	Customer 3075 has never been charged in NSW and has not been the defendant on an enforceable AVO. However, Customer 3075 is subject of numerous unproven reports relating to covert tracking and sexual assault of children.
Customer 1215	10 (9 magnetic)	Customer 1215 is the defendant on an enforceable ADVO and has a serious violent criminal history, as well as involvement in organised crime activity in NSW and interstate.
Customer 1087	10 (All magnetic)	Customer 1087 has no criminal history, although the Commission identified highly suspicious behaviour indicative of serious sexual offending. Customer 1087 is now under active criminal investigation.
Customer 2810	9 (All magnetic)	Customer 2810 is a close associate of a high-level member of an OMCG. Further enquiries identified that Customer 2810 purchased at least 12 more magnetic tracking devices and numerous listening devices since 2020.
Customer 2340	8 (All magnetic)	Customer 2340 is the defendant on an enforceable ADVO. They purchased devices from multiple retailers under fictitious names, consistent with an attempt to conceal their activities.

The Commission also found that customers who purchased a higher number of tracking devices presented significantly elevated criminal risk. Over 40% of the top 100 customers (based on the number of devices purchased) were known to the NSW Police Force in relation to domestic violence, compared to 25% of the entire customer base. The top 100 customers were also twice as likely to have been the defendant on an AVO, twice as likely to have been charged with a domestic violence offence, and more than twice as likely to be known for SOC offending. Of interest, every known customer who conducted seven or more purchases of magnetic tracking devices had an adverse record in NSW Police Force holdings.[28]

[28] This finding is based on the definition of 'relevant adverse reporting' defined above.

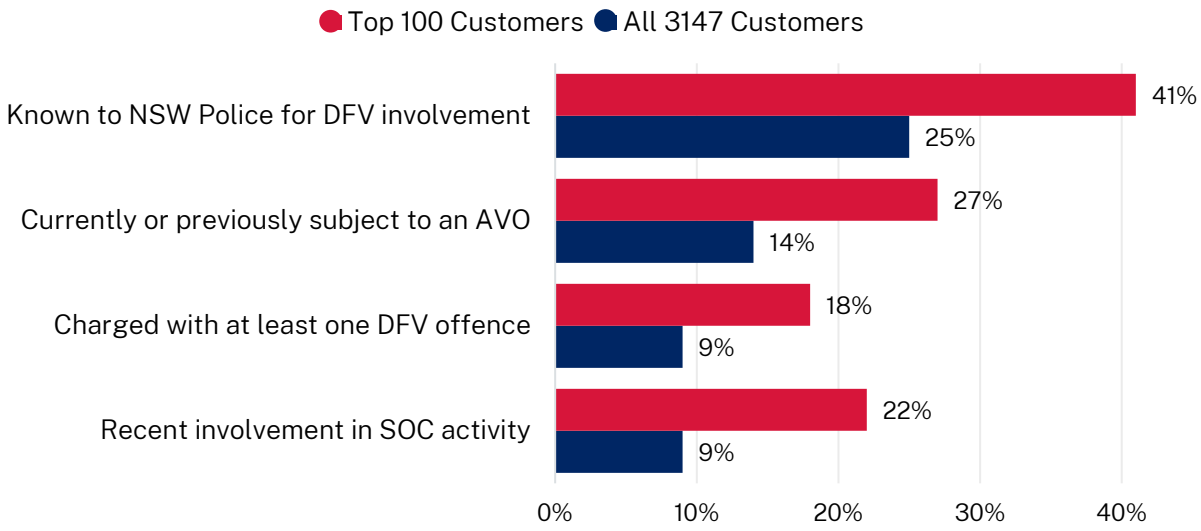


Figure 5: Variation in NSW Police Force reporting of top 100 customers vs. all customers

6 The private investigation and 'spy store' industries

Private investigators[29] and specialist 'spy stores'[30] sell surveillance services and devices to a range of clients. Several operators in this industry advertise covert and discreet surveillance options, making them appealing to DFV perpetrators and other individuals seeking to deploy unlawful surveillance.

> The Commission identified private investigators and specialist 'spy stores' that illegally deploy tracking devices and recklessly promote covert surveillance of intimate partners.

While the Commission did not find evidence that illegal or reckless conduct is pervasive within the industry, a thorough review of the industry was not within the scope of the investigation. The Commission interviewed some private investigators who expressed their disapproval of competitors and counterparts who deployed devices unlawfully, suggesting that this conduct was the exception rather than the norm. Indeed, some private investigators also provide services to DFV victims, including locating and removing surveillance devices deployed against them by offenders.

Nonetheless, it is clear that operators who break the law, or encourage customers to use surveillance devices unlawfully, generally do so openly and without disruption.

6.1 Irresponsible sales practices

Open-source searches of phrases relating to 'private investigators', 'spy stores', and 'cheating partners', return an array of companies that sell investigative services and surveillance devices. It is evident that 'infidelity investigations' are core business for some private investigators operating in NSW.

Private investigators and 'spy stores' also sell tracking devices, hidden cameras, listening devices, radio frequency detectors (commonly known as 'bug detectors'), and phone and computer spyware. These products are often advertised for use in covert monitoring of vehicles and people. A particular drawcard of 'spy stores' is that they sell surveillance devices disguised as household items.

The Commission found that providers often failed to caution customers that it is unlawful to use tracking, listening, and optical devices to monitor or record another person without their consent. Even when such cautions were included, they were often in fine print and incongruent with promotional material encouraging 'covert' and 'discreet' use of surveillance devices.

[29] Defined in section 4 of the *Security Industry Act 1997* (NSW) as a person who is employed or engaged for the purpose of investigation or surveillance of other persons.

[30] 'Spy stores' are businesses that sell gadgets and software used for covertly monitoring other people. They are not specifically regulated and are only required to hold a security licence if they sell certain items deemed to be 'security equipment' under the *Security Industry Act 1997* (NSW) *and the Security Industry Regulation 2016* (NSW). Tracking devices do not fall under the definition of security equipment.

The offering of covert surveillance devices makes these businesses appealing to individuals seeking to monitor or record other people without their knowledge. While some products have genuine uses, such as business, home, and personal security, they are exploited by perpetrators of domestic abuse and control.

Case Study 11

The Commission identified a private investigation company that sold over 200 tracking devices across Australia in 2023. Almost half were sold to customers based in NSW. The company's brochure for the tracking devices promotes covert tracking of intimate partners and does not caution that these activities are illegal if consent is not obtained.

The tracking devices were pre-installed with registered SIM cards, allowing customers to avoid using a SIM card subscribed in their own details. The company offered discreet delivery options, with 27 deliveries conducted via a rideshare app to grocery stores, petrol stations, post offices, and a hardware store.

One in four of this company's NSW-based customers were known to the NSW Police Force in relation to DFV incidents, including six defendants on enforceable AVOs. Five customers purchased tracking devices under names that appeared to be fictitious.

The Commission does not suggest that the company knew or should have known of the criminal histories of their customers, but does allege that their sales and marketing practices attracted this type of offender.

Case Study 12

A 'spy store' based in Sydney encourages customers to *'shop by concern'*, with one concern being *'suspect a partner is cheating?*'. The website invites users to complete a questionnaire which asks for their intentions and offers guidance on which products are most discreet.

The suggested items for customers seeking to catch cheating partners include GPS tracking devices, hidden cameras, listening devices, as well as an 'infidelity kit' that purports to be able to identify semen on any item of clothing in five minutes. When customers click on GPS tracking devices, they are taken to a page that explains how the device works but are not cautioned that purchasing tracking devices to monitor other people without their consent is a criminal offence.

The same store also sells spyware that can be covertly installed on Android phones. The spyware is marketed as 'Android Parental Monitoring Software', and includes live location tracking, keystroke logging, and remote monitoring of installed applications, internet history, images, and videos. The webpage contains 'legal considerations', which state that 'monitoring a device you own or have permission to monitor is legal', although 'monitoring someone else's device without consent is illegal'. Incongruently, one of the advertised drawcards of this spyware is that it can be covertly housed on the target's phone, by appearing as an innocuous Android OS Updater icon on the home-screen.

6.2 Private investigators and 'spy stores' servicing customers with criminal history

Private investigators and 'spy stores' do not have any requirement to conduct due diligence on customers prior to selling investigative services or surveillance devices. While operators may have risk mitigation or due diligence processes, these are currently implemented at the discretion of each operator. There is no enforceable industry standard for conducting due diligence, nor any criminal offence for recklessly supplying surveillance devices or services to dangerous clients. In fact, it is likely some private investigators remain wilfully blind to their client's criminal involvement and intentions.

The result of this lack of regulation is that private investigators and 'spy stores' provide services to individuals with a criminal history. The Commission is aware of two instances of private investigators who serviced customers with full knowledge of the clients' criminal intentions or associations.

The Commission analysed records of 456 sales of tracking devices by private investigators and 'spy stores' conducted since the start of 2023. From these sales, a total of 353 customers were recorded on the COPS database. Nearly 40% of these customers were known to the NSW Police Force for DFV or SOC activity.

> Nearly 40% of customers who purchased tracking devices from private investigators and 'spy stores' were known to the NSW Police Force for DFV or SOC activity.

Analysis of sales records provided by a Sydney-based 'spy store' identified that the business regularly sold items to customers who exhibited highly suspicious purchase behaviour. This included high volume repeat customers, as well as customers who purchased a range of covert tracking, listening, and optical devices in the same transaction. One domestic violence perpetrator purchased six magnetic tracking devices across six transactions between July 2023 and December 2023, before being charged under the SD Act in early 2024. A total of 31 sales by the business involved the purchase of a tracking device alongside other surveillance or counter-surveillance devices.

> A 'spy store' sold six magnetic trackers to a DFV perpetrator between July 2023 and December 2023. The customer was charged under the SD Act with unlawful use of tracking devices in January 2024.

Private investigators who specialise in infidelity investigations have been used by DFV perpetrators seeking to locate or monitor their current or former intimate partners. The following case study was provided to the Commission by the NSW Domestic Violence Death Review Team:

Case Study 13

A male offender had a history of engaging private investigators to conduct surveillance of former partners and his children. In July 2010, the offender hired a private investigator to locate his adult daughter. The investigator identified her current name and residential address, and provided this information to the offender who proceeded to stalk her. In December 2016, the offender hired a private investigator to establish whether his partner (the mother of the two children) had commenced a new relationship. The offender soon after began stalking his partner at an exercise studio, likely assisted by information provided by the private investigator. The offender had an extensive history of domestic violence against numerous prior partners and his children.

In July 2018, the offender shot and killed his two school-aged children at the home where they lived with their mother in metropolitan NSW.

The Commission also identified three cases where private investigators and 'spy stores' provided guidance, customer support, and device repairs to customers who were seeking to use surveillance devices for domestic violence or drug-related activity. In at least one case, the operator was aware that the customer intended to use the surveillance device unlawfully.

Case Study 14

A female victim approached the NSW Police Force after finding a magnetic GPS tracking device affixed to her vehicle. The victim reported being repeatedly contacted by her ex-partner, who was seeking to find her location after she had moved with the assistance of a DFV organisation. However, this contact had recently stopped, indicating that the offender found another way to monitor her location. NSW Police Force officers identified that the tracking device was being monitored by the offender and had been purchased from an Australian 'spy store'. The store had communicated with the offender on at least 10 occasions, including to discuss how to operate the device.

The offender was charged under the SD Act for the illegal use of a tracking device and was sentenced to an Intensive Correction Order.

The Commission identified at least three private investigators who have illegally deployed tracking devices as part of their investigative services. Private investigators who engage in such conduct are highly likely aware that their conduct is illegal but do so for convenience and to achieve a competitive edge.

Case Study 15

A private investigator was hired by a client to provide a range of protection and surveillance services. The client was affiliated with a Sydney-based OCN and paid the private investigator to conduct surveillance on various individuals. As part of the services provided, the private investigator installed a tracking device on the vehicle of a person known to the client. The investigator provided daily updates to the client, including location data from the tracking device and physical surveillance logs. Available information suggests the private investigator made attempts to obtain a SIM card subscribed in fraudulently obtained details to install in the tracking device. The investigator has since been charged under the SD Act.

Finding 5

Some private investigators and 'spy stores' promote the illegal use of surveillance devices and offer illegal surveillance services to customers.

6.3 Licensing and regulation of private investigators and 'spy stores'

Private investigators are regulated by the NSW Police Force Security Licensing & Enforcement Directorate (SLED), which administers the *Security Industry Act 1997* (NSW) (Security Industry Act) and the *Security Industry Regulation 2016* (NSW) (Security Industry Regulation). They are required to hold a Class 2E (Private Investigator) security licence in order to advertise or carry out paid investigative activities and must be employed by a Master Licence holder. Private investigators do not have any special authority and cannot engage in any activity that would be illegal for an ordinary civilian, including the deployment of surveillance devices to monitor a person without consent.

Security operators, including private investigators, are subject to general eligibility requirements. Eligibility can be impacted by several factors, including criminal history and prior dismissal from a police force on the grounds of integrity. For private investigators, an offence under the SD Act is a prescribed offence. A security licence can also be refused on discretionary grounds, including if granting the licence would be contrary to the public interest, or if the applicant is assessed to not be a fit and proper person.

Tracking devices and other household surveillance devices are not considered security equipment under the Security Industry Act and the Security Industry Regulation, and therefore the sale of these devices is not classed as a security activity in NSW. 'Spy stores' and other businesses that sell the types of surveillance devices referenced in this report are therefore not required to be licensed, or adhere to any certification or compliance regimes.

Recommendation 3

Having regard to the finding that some private investigators and 'spy stores' promote the illegal use of surveillance devices and offer illegal surveillance services to customers, Government ensure that the legislative and regulatory changes in **Recommendations 4 and 5** below are particularly applied to these industries.

7 Limitations and opportunities in the current legislative framework

7.1 Charge data under-represents actual offending

The number of charges laid under the SD Act significantly under-represents the true extent of offending relating to the criminal use of tracking devices. Only 34 offenders were charged with SD Act offences relating to tracking devices in 2022 and 2023 – 17 offenders each year.

The low charge rate is incongruent with the evidence base provided in this report detailing the extensive criminal use of tracking devices. In this investigation, the Commission found tracking devices are frequently used to facilitate organised crime violence, drug trafficking, and domestic violence (**Findings 1 and 2**). The Commission also identified 1156 adversely known individuals who have purchased tracking devices since the beginning of 2023 (see **Section 5.2**). Of these individuals, the Commission deemed 391 to be high-risk, including some who were subject to previous reporting regarding unlawful use of tracking devices. Only two of these high-risk individuals have been charged under the SD Act, both in 2024.

Beyond this evidence base, this report has highlighted qualitative reasons for the under-detection and under-prosecution of criminal offending involving tracking devices. These include:

- the under-detection of offending due to the concealability of tracking devices and the fact that criminal tracking is usually intended to be covert;
- the under-reporting of technology-facilitated abuse in a DFV context (see **Section 4.4**);
- challenges with gathering sufficient evidence due to a lack of licensing and regulation within the industry (see **Section 7.2** below); and
- the requirement to obtain Attorney General consent to institute charges under the SD Act, which may present a barrier to charging (see **Section 7.3.1** below).

Criminal use of a tracking device can also form part of the brief of evidence for another primary offence and may not always be prosecuted under the SD Act. Most instances of organised crime violence reviewed for the purpose of this investigation resulted in prosecutions for the primary offence only. The Commission also identified 21 examples from 2022 and 2023 where an offender used a tracking device in the course of domestic violence-related stalking or intimidation that was prosecuted under section 13 of the *Crimes (Domestic and Personal Violence) Act 2007* (NSW), but not under the SD Act. It is not possible to assess the true extent to which tracking devices are detected during investigations into other offences.

Finding 6

Charges laid under the *Surveillance Devices Act 2007* (NSW) significantly under-represent the true extent of offending involving tracking devices.

7.2 Licensing and regulation

There is no regulatory framework in NSW governing the sale of tracking and other surveillance devices. The SD Act does not establish any licensing or record keeping requirements for sellers of surveillance devices, beyond the prohibition in section 13 of the SD Act against supplying, or offering to supply, a surveillance device with the intention of it being used in contravention of the SD Act. While the Security Industry Act requires sellers of security equipment such as alarms and Closed Circuit Television (CCTV) systems to hold a security licence, tracking and other surveillance devices do not meet the definition of 'security equipment' provided in the Security Industry Regulation.

Sellers of surveillance devices are not required to record customer details, itemised sales records, or device identifiers. While most retailers approached by the Commission recorded customer details and sales records for invoicing purposes, these records had varying degrees of accuracy. Retailers generally did not require customers to produce identification documentation, and sometimes recorded partial or no customer details.

None of the retailers approached by the Commission recorded device identifiers, such as the serial number or IMEI number. There also appeared to be a lack of understanding about the difference between a serial number and an IMEI number. While both numbers uniquely identify the device, the IMEI number follows an international telecommunications standard and can be used by law enforcement to collect intelligence and evidence for investigations and prosecutions. The SIM card installed in a tracking device can also hold information relevant for investigative and evidentiary purposes; however, retailers do not commonly sell SIM cards along with tracking devices.

Case Study 16

A tracking device was seized by NSW Police Force officers during a search warrant at the home of an offender who was charged in relation to an organised crime murder. The NSW Police Force also located an instruction manual for the tracking device which contained the logo for a 'spy store' run by a Sydney-based private investigator. The Commission approached the private investigator, who was unable to produce a record of purchase for the device.

In several recent organised crime murders and kidnappings where tracking devices were recovered by law enforcement, investigators were unable to identify the retailer or the purchaser of the tracking devices. In other matters where OCNs were known to use tracking devices in criminal offending, the devices could not be identified or located, limiting proactive investigative opportunities.

Case Study 17

A tracking device was used to plan an attempted shooting murder in 2023. During the investigation, NSW Police Force officers seized the tracking device, and the Commission and NSW Police Force undertook extensive enquiries to identify where and by whom the device was purchased. Despite significant intelligence collection and the use of NSW Police Force and Commission powers, these enquiries failed to identify the retailer who sold the device.

Retailers have no due diligence or 'know your customer' requirements, nor do they have any obligation or specific mechanism to report suspicious purchases to authorities. There are no barriers to retailers making police reports, but equally, no compulsion– and the Commission did not identify any instances where a report was made. A requirement for businesses who sell tracking devices to be registered, to record device identifiers and customer details, and to report suspicious purchases would improve the ability of law enforcement agencies to investigate and prosecute offenders who unlawfully use surveillance devices.

Finding 7

Law enforcement efforts to investigate criminal offences and locate tracking devices used by high-risk individuals are frustrated because:

a. there are no licensing or registration requirements for suppliers of tracking devices, and suppliers do not have any due diligence, data collection, or mandatory reporting obligations;

b. there are no licensing or registration requirements for purchasers or users of tracking devices in NSW; and

c. identifiers of tracking devices (for example, the IMEI) are not required to be recorded prior to sale and suppliers do not record such data.

Recommendation 4

Government regulate the sale of surveillance devices, including through:

a. licensing for suppliers of surveillance devices;

b. recording of device identifiers;

c. recording of customer details;

d. mandatory reporting of suspicious purchases.

7.3 Opportunities to strengthen legislation

7.3.1 Requirement to obtain the consent of the Attorney General to institute prosecutions under the SD Act

Section 56 of the SD Act stipulates that the written consent of the Attorney General is required to institute prosecutions under the Act. This approval has been delegated to the Director of Public Prosecutions (DPP). On 6 June 2024, the NSW Parliament passed the Bail and Other Legislation Amendment (Domestic Violence) Bill 2024 (NSW) which removes the requirement of Attorney General consent for proceedings for an offence against section 9 of the SD Act (relating to tracking devices), where the offence is domestic violence related. Attorney General the Hon. Michael Daley MP outlined the rationale for this proposed amendment in his Second Reading Speech, noting technology as a "critical component" of the stalking behaviour exercised by perpetrators of domestic abuse.[31]

[31] Legislative Assembly Hansard - 15 May 2024 - Proof (nsw.gov.au), last accessed 17 June 2024.

This amendment, which is yet to commence, is a significant step toward strengthening the SD Act. However, it does not encompass any tracking device offence that does not relate to domestic violence, nor any offence involving other surveillance devices such as optical or listening devices.

Only 62 of the 219 offenders charged under the SD Act between 2010 and 2023 would have met the criteria outlined in the June 2024 amendments for removal of Attorney General consent. This means that the NSW Police Force would still have been required to seek consent to institute a prosecution in 72% of these cases, if they had been prosecuted after the commencement of the June 2024 amendments. This includes most of the case studies provided in this report.

Obtaining the Attorney General's consent requires the prosecuting officer to submit a brief of evidence to the DPP for approval. This process can cause a delay in instituting SD Act charges and may contribute to the low charge rate.

7.3.2 Use of tracking devices to facilitate serious criminal activity

This investigation identified frequent use of tracking devices to facilitate serious violence and drug trafficking offences. This often constitutes an offence under section 9 of the SD Act.

Even when the use of a tracking or other surveillance device does contravene the SD Act, offences under the SD Act are not tiered according to the severity of the criminal activity facilitated by the surveillance device.

Consideration should be given to prohibiting the installation, use, maintenance, or monitoring of a tracking or other surveillance device with the intention of facilitating serious criminal activity of any type, including both organised crime and domestic violence. This should carry a higher maximum penalty than the standard offences established in the SD Act.

7.3.3 Monitoring of tracking devices

The SD Act does not specifically prohibit the monitoring of a surveillance device for unlawful purposes. Monitoring of a tracking or other surveillance device can form a substantial part of criminal offending. OCNs planning acts of violence may assign a particular syndicate member to monitor the location of a tracking device that someone else installed.

Meanwhile, some perpetrators of domestic violence endeavour to constantly monitor their intimate partners, sometimes over extended periods of weeks or months. In these instances, the severity of the offence should be associated with the frequency and length of monitoring of the device, rather than the initial act of installing the device. In some circumstances, consent may have been provided for the initial installation of a device but then withdrawn during the period of monitoring. In such circumstances, it is unclear whether the existing offences of 'installing', 'using', or 'maintaining' a device would be sufficient to charge and prosecute offenders.

Similarly, certain surveillance applications – such as in-built vehicle location systems – may not be 'installed', but rather accessed and monitored. The monitoring of these applications will amount to coercive control from 1 July 2024, although only in circumstances where the victim is a current or former intimate partner of the offender- see **Section 4.3**.

Prohibiting the monitoring of surveillance devices for unlawful purposes would better capture malicious tracking activity in broader domestic violence and organised crime settings.

7.3.4 Reckless supply of surveillance devices

There is currently no offence for reckless supply of a tracking or other surveillance device in NSW. Section 13 of the SD Act prohibits supply of a surveillance device, but requires proof that the offender *intended* for the surveillance device to be used in contravention of the SD Act.

The Commission identified numerous examples of tracking devices being transferred in covert exchanges that were consistent with criminal use. This included, for example, the use of 'dead drops' where items are left in a particular location by one party and collected anonymously by another. In these examples, even if the supplier was not specifically aware of the intended use of the device, they would have recognised that the circumstances surrounding the handover were not consistent with lawful use.

Establishing an offence that prohibits the supply of a surveillance device with recklessness as to whether the device will be used unlawfully would counteract the measures adopted by OCNs to distance themselves from their offending, and would capture third parties who assist and enable serious offending to occur. Furthermore, the current legislation does not address irresponsible or reckless advertising and sales practices by retailers. For example, **Chapter 6** identified that some private investigators and 'spy stores' sell tracking devices that they advertise for use in covert tracking. While these providers would not be aware of the specific intentions of each customer, the nature of their promotional material is consistent with illegal use of their product.

7.3.5 Causing the installation, use or maintenance of a tracking device

Section 9 of the SD Act only prohibits the installation, use, and maintenance of a tracking device without consent. The Commission is aware of several examples – including at least one organised crime murder – where an individual paid or instructed another person to install a tracking device. The current legislation may preclude prosecution of the individual who caused the device to be installed.

Consideration should be given to the creation of an offence to prohibit any act that causes a surveillance device to be installed, used, maintained, or monitored without consent, including directing or instructing another person to do so.

Recommendation 5

Government strengthen legislation to:

a. remove the requirement to obtain the Attorney General's consent to institute prosecutions under the *Surveillance Devices Act 2007* (NSW), beyond the amendment contained in the Bail and Other Legislation Amendment (Domestic Violence) Bill 2024 (NSW);

b. prohibit the use of a surveillance device to facilitate serious criminal activity;

c. prohibit the use of a surveillance device to facilitate a domestic violence-related offence;

d. prohibit the monitoring of a surveillance device alongside the use, installation, and maintenance;

e. prohibit the supply of a surveillance device with *recklessness* as to whether it will be used unlawfully, such as encouraging unlawful use of tracking devices in advertising material; and

f. prohibit any activity that causes a surveillance device to be installed, used, or maintained without consent (including instructing another person to do so).

7.4 Other opportunities to reduce criminal use of tracking devices

This investigation has identified individuals who purchased tracking devices while subject to community-based sentences or civil orders such as AVOs.[32] Tracking devices were sometimes purchased in the days following an interaction with NSW Police Force officers in relation to a domestic violence event (see **Section 5.6**). Furthermore, the Commission found that of the 79 offenders who were charged with a domestic violence-related tracking device offence under the SD Act between 2010 and 2023, over one third (27) were the defendants on ADVOs intended to protect the victim of the offence.

Case Study 18

A female victim separated from her male partner of two years. During the relationship, the offender demanded to know where the victim was at all times, and displayed behaviour consistent with coercive control, including threatening animals and threatening self-harm. After separating, the offender continued to harass the victim and an ADVO was sought by the NSW Police Force to protect the victim. Shortly after, the victim identified a magnetic GPS device attached to her vehicle.

Investigation by the NSW Police Force confirmed her male partner was monitoring the device. The NSW Police Force identified that the offender checked the location of the GPS tracking device more than 500 times in a 7-day period. The offender was charged under the SD Act and was also charged with contravening the ADVO. He received a 12-month Community Correction Order and has since continued to offend against the victim.

There is currently no legislated requirement to address the purchase, possession, or use of tracking devices within AVO, bail, parole, or community-based sentence conditions. While such conditions relating to tracking and other surveillance devices could still be applied at the discretion of the relevant Court or Tribunal, the Commission is not aware of this occurring on a regular basis.

Including specific conditions relating to tracking and other surveillance devices would mitigate the risk presented by individuals who are subject to civil orders or serving criminal sentences in the community. It would also provide more scope for intervention against individuals who continue to purchase and illegally use these devices while subject to orders.

Case Study 19

A male offender was charged under the SD Act in relation to the tracking of his former partner. The offender had installed two tracking devices on the victim's vehicle, which she provided to the NSW Police Force. The victim also reported that over the previous two years, she had discovered and removed over 15 tracking devices that had been affixed to her vehicle. Throughout the period of offending, the offender was the defendant on an ADVO intended to protect the victim.

[32] Community-based sentences refer to court orders which allow offenders to carry out their sentence within the community, and not in a prison, such as Intensive Correction Orders and Community Correction Orders.

The SD Act charge was withdrawn, although the offender was sentenced to an 18-month Community Correction Order for contravening an ADVO. The offender had previously been charged with domestic violence offences relating to the use of a tracking device, for which he received a fine.

He has since been convicted of further domestic violence offences and is currently serving both a Community Correction Order and an Intensive Correction Order.

Opportunities to reduce criminal use of tracking devices are outlined in Recommendation 2, as detailed in **Section 5.6.**

8 Analysis of charges laid under the *Surveillance Devices Act 2007* (NSW)

8.1 Relevant offences

There is a general prohibition against the installation, use, and maintenance of tracking devices, provided in subsection 9(1) of the SD Act:

> *A person must not knowingly install, use or maintain a tracking device to determine the geographical location of—*
>
> *(a) a person—without the express or implied consent of that person, or*
>
> *(b) an object—without the express or implied consent of a person in lawful possession or having lawful control of that object.*

The SD Act sets out similar prohibitions regarding listening, optical, and data surveillance devices.

There is also a general prohibition against the manufacture, supply, and possession of surveillance devices provided in subsection 13(1) of the SD Act:

> *A person must not—*
>
> *(a) manufacture, or*
>
> *(b) supply or offer to supply, or*
>
> *(c) possess,*
>
> *a data surveillance device, listening device, optical surveillance device or tracking device with the intention of using it, or it being used, in contravention of this Part.*

The offences regarding the installation, use, maintenance, manufacture, supply, and possession of surveillance devices all carry a maximum penalty of 5 years imprisonment.

8.2 Charges laid under the *Surveillance Devices Act 2007* (NSW)

Between 2010 and 2023, the NSW Police Force charged 219 offenders under the SD Act, with a total of 438 charges laid.[33] Around 30% of these charges related to the unlawful use of tracking devices, as defined in Section 9 of the SD Act. A breakdown of charges is provided below.

There has been a general increase in the number of charges laid over time. The introduction of the Apple AirTag into the Australian market in April 2021 almost certainly contributed to this increase, with 14 offenders charged in relation to unlawful use of AirTags since this time.

[33] The Commission reviewed data since 2010 due to limitations regarding access to data from before this time.

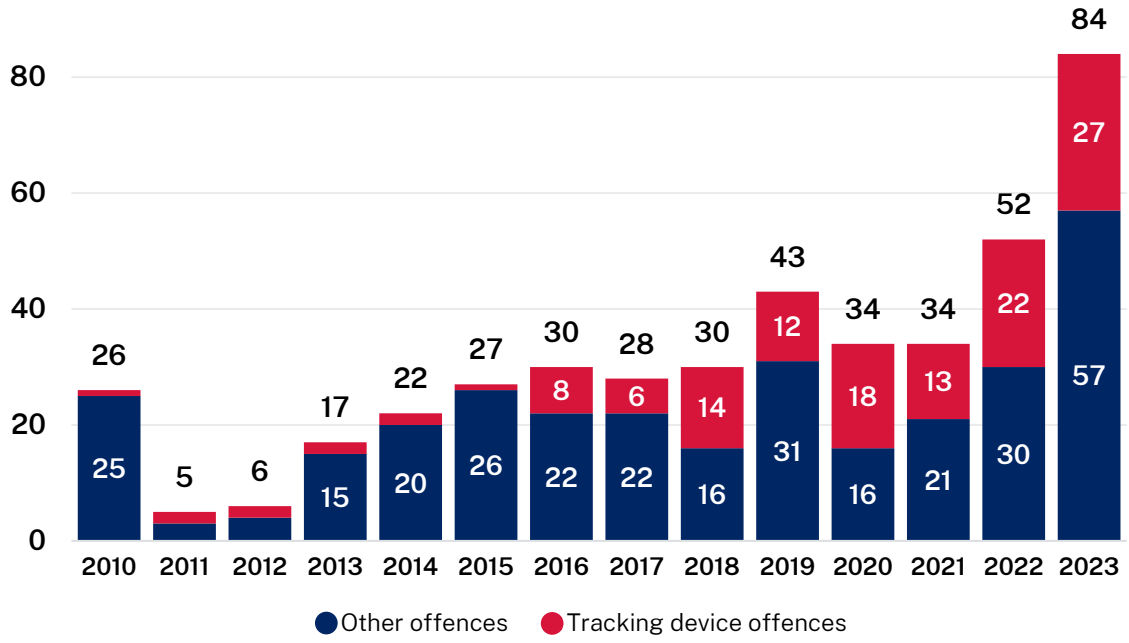


Figure 6: Charges laid under the SD Act between 2010 and 2023

8.3 Charge breakdown

The following table provides a breakdown of the 438 charges laid under the SD Act between 2010 and 2023.

Section	Law Part Code	Prescribed Law Part Title	Charges Laid
9(1)(a)	66198	Install/use tracking device to locate person without consent	**92**
7(1)(a)	66194	Install or use etc listening device to record etc private conversation not party to	**78**
7(1)(b)	66195	Install or use etc listening device to record private conversation party to	**64**
10(1)(a)	66200	Install/use optical surveillance device – entry without consent	**59**
12(1)	66203	Possess conversation obtained by surveillance devices	**43**
9(1)(b)	66199	Install/use tracking device to locate object without consent	**38**
11(1)	66202	Publish etc conversation obtained by surveillance devices	**25**

Section	Law Part Code	Prescribed Law Part Title	Charges Laid
13(1)(c)	66206	Possess supply surveillance devices intend unlawful use	**17**
8(1)(b)	66197	Install/use optical surveillance device – interfere with vehicle/premises without consent	**12**
40(1)	66208	Intentionally etc publish or communicate protected information	**7**
8(1)(a)	66196	Install/use data surveillance device – entry without consent	**2**
13(1)(a)	66204	Manufacture surveillance devices intend unlawful use	**1**

8.4 Tracking device charges

Between 2010 and 2023, the NSW Police Force charged 96 offenders with offences relating to the unlawful use of tracking devices under the SD Act.[34] One of these offenders was charged on two occasions – once in relation to an organised crime event, and once in relation to domestic violence. This brought the total number of criminal events to 97.

The Commission reviewed each criminal event to assess the circumstances surrounding the crime. This revealed a significant cohort of domestic violence perpetrators. Of the 97 criminal events, 79 were DFV-related and 14 were related to organised crime. The remaining four did not fall into either category. Further insights regarding these offenders are provided below.

One additional offender was charged in 2010 with the supply of a tracking device. Since then, there has not been a single prosecution for supplying a tracking device in NSW.

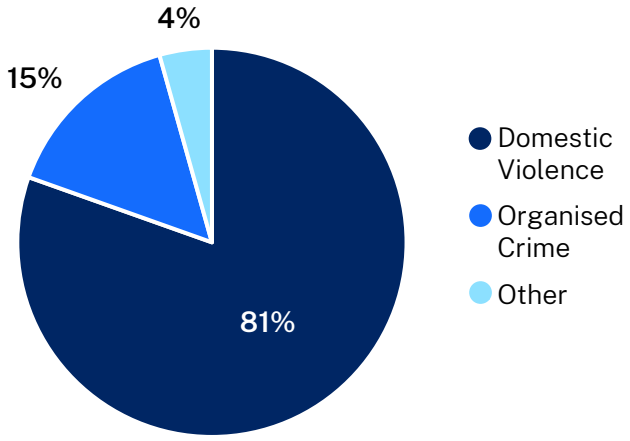


Figure 7: Crime type relating to tracking device charges

Magnetic GPS tracking devices were the most common type reported in the events, followed by Bluetooth tags (mostly AirTags), and then hardwired GPS devices. The device type was not specified in around one-third of cases, although in most of these instances the corresponding charge narrative was consistent with the device being a magnetic GPS tracking device.

[34] These offenders were all charged under section 9 of the SD Act.

Offender insights

- **75%** had been charged on at least one other occasion.
- **65%** were adversely recorded in NSW Police Force intelligence holdings.
- **One in three** had known links to OCNs.

Tracking device type	# of events
Magnetic GPS device	31
Unknown	31
Bluetooth tag or tile	16
Hardwired GPS device	14
Other electronic device[35]	5

8.5 Outcomes and sentencing

The NSW Bureau of Crime Statistics and Research (BOCSAR) provided outcomes and sentencing data regarding 109 charges under section 9 of the SD Act that were finalised between 2007 and 2023: 46% were withdrawn, 40% were proven, and 3% resulted in a not guilty finding. The remaining 8% were dismissed or disposed of by the Court without any determination being made regarding guilt.

Of the 27 offenders where a finalised tracking device charge was the principal proven offence,[36] only three resulted in a custodial sentence.

[35] This included items which have location tracking settings but are not solely GPS tracker devices, such as phones or tablets.

[36] A more detailed explanation of how a principal offence is determined can be found on BOCSAR's website, https://www.bocsar.nsw.gov.au/Pages/bocsar_court_stats/court_glossary.aspx#P. The principal proven offence is defined as the charge which received the most serious penalty.

9 Genuine use and availability of tracking devices

While this report addresses the criminal use of tracking devices, the Commission found that they also have substantial genuine use. This section identifies the main genuine uses of tracking and other surveillance devices and provides an overview of their availability in NSW.

9.1 Genuine use of tracking devices

Tracking devices have a range of genuine uses, including fleet management, asset protection, and personal security. Businesses in the logistics, transport, mining, and car hire industries commonly use tracking devices for real-time fleet management, theft recovery, driver conduct and safety, and managing maintenance requirements.

Tracking devices are also routinely purchased by small-to-medium sized businesses and individual customers to secure vehicles, motorcycles, and machinery. Tracking devices are therefore often sold as 'anti-theft' devices. These devices may also be purchased for personal safety, in particular for individuals driving in unfamiliar or rural locations.

Hardwired tracking devices are generally more reliable than battery-powered magnetic devices and are the recommended choice for genuine use. Hardwired devices offer more reliable location data and do not have to be regularly replaced or recharged. Furthermore, hardwired devices often have additional features including engine immobilisation and vehicle diagnostics. Battery-powered devices are only preferrable when hardwiring is not an option, such as for trailers or certain types of machinery, or when the device is only needed for a short period of time. Reflecting this preference, the Commission found that most major automotive parts retailers no longer sell battery-powered tracking devices.

Bluetooth tags and tiles, such as Apple AirTags, have substantial mainstream use for tracking personal items such as keys, wallets, and luggage. Tags and tiles are also sometimes marketed as personal safety devices for children and elderly people. There is also a significant market for pet tracking tags and animal collars with in-built tracking capabilities. A growing market also exists for fitness trackers, which include GPS location capabilities that allow athletes to track speed and distance travelled.

9.2 Availability of tracking devices

GPS tracking devices are widely accessible in NSW and can be purchased through local and overseas retailers. Locally, tracking devices can be purchased from electronics stores, automotive parts stores, private investigators, 'spy stores', and security equipment businesses. Some of these retailers operate as online-only businesses.

Large online marketplaces and e-commerce platforms also sell tracking devices, including Gumtree, eBay, Facebook Marketplace, Amazon, and Ali Baba. While each of these platforms vary, most facilitate the sale of items from overseas sellers to local customers. Devices can also be purchased directly from some overseas manufacturers, although these brands are also widely available on online marketplaces.

The price of tracking devices varies substantially between retailers with devices being sold for anywhere between $30 and $350. Some tracking devices are sold cheaply but require a paid subscription to access the online platform used to monitor the location of the device.

Open-source searches identified a substantial number of businesses offering fleet management packages that include hardwired GPS tracking devices and sophisticated monitoring platforms. These businesses likely appeal to larger companies that manage a high volume of vehicles and/or machinery, and were not of interest to this investigation.

9.3 Other common surveillance devices

Optical and listening devices such as covert cameras and voice recorders are also widely available in NSW. They may be purchased for genuine reasons including to secure residential and business premises. These devices can be purchased from online marketplaces, e-commerce platforms, private investigators and 'spy stores'.

10 Appendix A – Investigation methodology

The Commission collected information through traditional law enforcement investigative methods, reviewed open-source and academic material, and deployed statutory powers including production notices and coercive hearings. The Commission also applied data analytics techniques to draw insights from datasets obtained during the investigation.

10.1 Review of existing material and environmental scanning

The Commission reviewed data collected from its own criminal investigations and also had access to information from the NSW Police Force, the Australian Transaction Reports and Analysis Centre (AUSTRAC), the Department of Home Affairs, and the Australian Federal Police. This information was obtained through existing access to external agency databases and requests for information. Most information was used to inform the Commission's contextual understanding of the matters under investigation. In cases where specific information was used in this report, authorisation was sought from the relevant agency.

The Commission also reviewed open-source material, including media reporting, academic literature, and existing legislative frameworks. This included substantial review of public reports regarding coercive control and technology-facilitated domestic abuse.

This investigation was also informed by open-source searches relating to tracking devices and other surveillance technology. The Commission reviewed hundreds of online listings for tracking devices to build an understanding of the functionality and genuine uses of these devices. This process provided significant insight into where and how tracking devices are purchased, as well as how they are advertised to prospective customers. This information was used to inform future data collection and offered the Commission insights into the current environment surrounding the availability and sale of tracking devices.

10.2 Consultation with law enforcement and industry bodies

The Commission consulted with a number of subject matter experts within industry and law enforcement. This included retailers, law enforcement investigators, government policy teams, and experts in technology-based domestic violence. These individuals provided unique insights regarding the availability and criminal use of tracking devices, and discussed limitations in the current legislative and regulatory framework surrounding tracking devices.

The Commission consulted with the NSW Police Force and other agencies to manage specific safety risks uncovered during this investigation. The Commission sent intelligence referrals to the Australian Criminal Intelligence Commission, Department of Home Affairs, NSW Healthcare Complaints Commission, Queensland Police Service, Queensland Crime and Corruption Commission and Western Australia Police Force. Some of these referrals resulted in criminal investigations that remain active.

10.3 Investigative powers

The following table summarises the Commission's use of statutory and other law enforcement powers during this investigation.

Legislation	Section and purpose	Number
CC Act	s 29: to obtain documents and things pertaining to an investigation by the Commission	33
CC Act	s 24: to summons a person to give evidence pertaining to an investigation by the Commission	8
TIA Act	s 178: historical data authorisations	62
TIA Act	s 180: prospective data authorisations	7

The Commission also interviewed people involved in, or directly associated with, OCNs in NSW. These individuals had specific knowledge about the use of tracking devices to further serious and organised crime. Their insights contributed to support the analysis in this report.

10.4 Data collection and analysis

The Commission issued 33 compulsory production notices to 31 entities. Twenty-two of these notices, issued to 20 retailers, specifically related to the production of tracking device sales data. These 22 notices required each recipient to produce to the Commission approximately 12 months of sales records of GPS tracking devices since 1 January 2023. Recipients included electronics stores, automotive parts stores, private investigators, 'spy stores', online marketplaces, and international online retailers.

The data was then analysed to identify customers who had purchased tracking devices. These customers were assessed against law enforcement databases, and a risk profile and referral option was generated for each customer.

10.5 Limitations

The most significant limitation, identified primarily in **Chapter 7**, is the absence of regulation around the sale and purchase of surveillance devices in NSW. This made it impossible for the Commission to obtain a comprehensive dataset of tracking device sales. The quality of data varied across retailers, as did the level of detail retained about customers and devices.

Since there are various genuine reasons to purchase tracking devices, there is often no way of easily identifying whether a particular individual purchased a device for genuine or criminal reasons. It is likely that some individuals who were flagged as 'high-risk' actually purchased tracking devices for genuine reasons. Equally, it is likely that some individuals who purchased tracking devices for criminal purposes were not identified during this investigation.

Due to the volume of potential data available, the Commission was deliberate about which retailers were approached, and what information was requested from each retailer. The Commission prioritised approaches to retailers that were known to have been used by, or assessed to be attractive, to criminals. The Commission targeted data collection around the types of devices that were most likely to be used to facilitate criminal offending. For example, the report lacks significant detail regarding the genuine use of hardwired tracking devices for fleet management purposes, because the Commission did not approach businesses that specialise in such solutions.

Along with limitations in the data provided by retailers, gaps were identified within law enforcement databases, including the absence of a mechanism to 'flag' instances where tracking or other surveillance device were used in a criminal offence or crime event.

11 Appendix B – Terminology and definitions

11.1 Terminology relating to charge data

The term 'charge' has different definitions across NSW government bodies. When a person is charged in NSW, they are provided with a Court Attendance Notice (CAN) which contains details of the alleged offence/s. The CAN includes a charge reference number that starts with the letter H, sometimes referred to as an 'H number'. Within the COPS database, each 'H number' is referred to as a single charge comprising of one or more offences. This terminology is generally adopted by law enforcement officers in NSW.

BOCSAR, who provide authoritative crime statistics for NSW, does not specifically measure H numbers and instead refers to each offence within an H number as its own 'charge'. To maintain consistency in public discussion, this report follows BOCSAR's terminology.

11.2 Definitions of surveillance devices

The following definitions are provided by the SD Act.

Surveillance device type	Definition
Tracking device	Any electronic device capable of being used to determine or monitor the geographical location of a person or an object.
Listening device	Any device capable of being used to overhear, record, monitor, or listen to a conversation or words spoken to or by any person in conversation, but does not include a hearing aid or similar device used by a person with impaired hearing to overcome the impairment and permit that person to hear only sounds ordinarily audible to the human ear.
Optical surveillance device	Any device capable of being used to record visually or observe an activity, but does not include spectacles, contact lenses, or a similar device used by a person with impaired sight to overcome that impairment.
Data surveillance device	Any device or program capable of being used to record or monitor the input of information into or output of information from a computer but does not include an optical surveillance device.

11.3 Referenced legislation

Full name of Act, Bill or Regulation
Bail Act 2013 (NSW)
Bail and Other Legislation Amendment (Domestic Violence) Bill 2024 (NSW)
Crime Commission Act 2012 (NSW) ('CC Act')
Crimes (Domestic and Personal Violence) Act 2007 (NSW)
Crimes Act 1900 (NSW)
Crimes Legislation Amendment (Coercive Control) Act 2022 (NSW)
Criminal Assets Recovery Act 1990 (NSW)
Security Industry Act 1997 (NSW) ('Security Industry Act')
Security Industry Regulation 2016 (NSW) ('Security Industry Regulation')
Surveillance Devices Act 2004 (Cth)
Surveillance Devices Act 2007 (NSW) ('SD Act')
Telecommunications (Interception and Access) Act 1979 (Cth) ('TIA Act')

11.4 Abbreviations

Abbreviation	Meaning
ANROWS	Australia's National Research Organisation for Women's Safety
ADVO	Apprehended Domestic Violence Order
AUSTRAC	Australian Transaction Reporting and Analysis Centre
AVO	Apprehended Violence Order
BOCSAR	NSW Bureau of Crime Statistics and Research
CAN	Court Attendance Notice
CCTV	Closed Circuit Television
COPS	Computerised Operational Policing System
DPP	Director of Public Prosecutions
DFV	Domestic and Family Violence
FPO	Firearms Prohibition Order
GPS	Global Positioning System
IMEI	International Mobile Equipment Identity
OCN	Organised Crime Network
OMCG	Outlaw Motorcycle Gang
WESNET	Women's Services Network
SIM	Subscriber Identity Module
SOC	Serious and Organised Crime