The Domestic and Family Violence GPS-enabled Electronic Monitoring Technology

EVALUATION REPORT

April 2019

Contents

Executive Summary

In 2015, the Special Taskforce on Domestic and Family Violence in Queensland (the Taskforce), provided its report, *Not Now, Not Ever: Putting an End to Domestic and Family Violence in Queensland* (the Taskforce Report) to the Premier. Recommendation 123 of the Taskforce Report was:

> *The Queensland Government trials the use of Global Positioning System (GPS) monitoring for high risk perpetrators of domestic and family violence*.

To progress implementation of this recommendation, the Taskforce advocated a trial approach to further explore the effectiveness of electronic monitoring in supporting victim safety. In August 2015, the Queensland Government released its response to the Taskforce Report accepting all the recommendations, including the commitment to explore options to monitor high risk perpetrators of domestic and family violence (DFV).

The Queensland Police Service (QPS), the Department of Justice and Attorney-General (DJAG), Queensland Corrective Services (QCS) and the Department of the Premier and Cabinet (DPC) adopted a joint approach to examine Recommendation 123. As part of its cross-agency commitment, the QPS agreed to test GPS-enabled electronic monitoring technology through a controlled trial in the context of simulated DFV scenarios.

It was agreed the testing of the technology should initially be carried out via simulated scenarios, as opposed to establishing a live trial, due to concerns around reliance on untested technological applications as a mitigating measure. Importantly, the trial design acknowledged the highly unpredictable and emotive nature of DFV crime, which needs to be contrasted with existing applications of GPS-enabled technologies to support community-based management for subject classes characterised by more stable risk profiles.

To complement the technology trial, the Government also committed to commissioning external research to explore the electronic monitoring of DFV perpetrators in a range of criminal law contexts, including bail, and probation and parole. The findings of the external research and evaluation of the controlled trial will help the Government to determine if it is appropriate to introduce a GPS-enabled electronic monitoring program for perpetrators of DFV. This evaluation report is the key output from the technology trial.

Importantly, the technology trial examined GPS-enabled electronic monitoring as a sole risk mitigation measure in the context of DFV offending. It should be noted that existing electronic monitoring strategies used by QCS do not rely on electronic monitoring alone as a risk mitigation strategy, rather it forms part of a robust case management and surveillance framework. The broader proactive communication between a monitoring service and the subject, individualised suitability assessments of a subject and their environment, field response components, support services to address the offending behaviour and the legislative framework, which would provide a comprehensive, community-based case management framework, in addition to electronic monitoring were not considered during the trial. Considerable caution needs to be exercised in making comparisons of the use of electronic monitoring in the DFV stimulated trials with other classes of electronic monitoring subjects within a more established management framework.

The purpose of this evaluation was to test the reliability and accuracy of contemporary GPS-enabled electronic monitoring technology within the context of DFV simulated scenarios.

The evaluation design employed a mixed methods approach, based on the collection and analysis of both quantitative and qualitative data sources.

The quantitative data comprised of administrative data extracted from the monitoring system and manual recordings of the physical locations of tracked persons in real-time according to each scenario. The qualitative data comprised of data coded from observations by officers conducting the trial and a review of relevant literature analysing the benefits, challenges and limitations regarding the operational use of GPS-enabled technology within a DFV context.

The technology was tested in various locations across Queensland through seven scenarios developed and enacted in each location to assess the effectiveness of the technology. The scenarios involved simulating real-world environments including a perpetrator approaching a fixed location frequented by a victim, chance encounters in unregulated public spaces, and 'stalking' the perimeters of a prohibited zone. A perpetrator subject to electronic monitoring will usually have conditions stipulated in their court order, so specific distances were applied for each zone examined as part of the trial. It should be noted that the size and configuration of zones as they are set in the system can impact results.

To assess the reliability of the tracking devices in detecting entry into a prohibited area (i.e. an exclusion zone, an interest zone or a victim-proximity zone), officers deliberately breached pre-programmed prohibited areas. Reliability was measured according to whether an alarm was activated at the monitoring system to alert the breaching of a zone. Some scenarios required just one alarm to activate (e.g. a GPS exclusion zone alert), whilst others required more than one alert to activate (e.g. a GPS exclusion zone alert, radio frequency beacon alert and/or victim-proximity zone alert).

Results in just over half the scenarios (51 percent) were found to be a success – that is, each alert activated as required according to the pre-programmed conditions of the scenario. About a quarter of the scenarios (23 percent) were found to be partially successful, meaning at least one alert, from a possible two, three, or four alerts, activated following the breaching of a zone. The remaining quarter of the scenarios (26 percent) failed, meaning no alert/s activated at all following the breaching of a zone. Based on these outcomes, findings show one in four breaches occurred with no alert activating at all and so the breach was wholly undetected. These results reflect the operational and technical outcomes recorded during field testing and may be inconsistent with experiences in other applications or situations.

An examination of how well the GPS-enabled technology tracked the movements of individuals imposed with a tracking device also indicated moderate levels of accuracy. There were multiple incidents of multi-path errors recorded in the raw data – that is, notable variances in the electronically tracked movements and the real route undertaken by the individual. It is unlikely GPS-enabled technology could be relied upon without other supporting evidence to fix the location of an individual at a particular time to a required evidentiary standard, but it may instead be acceptable if tendered as corroborating evidence.

When interpreting the results of the trial it is important to acknowledge the complexity of the tracking data that was captured and recorded on the monitoring system for interpretation purposes. This complexity was identified as a significant obstacle experienced by the QPS staff involved in the technology trial. GPS-enabled technology provides a great deal of information, however, understanding and interpreting this data requires specialised skills and an in-depth knowledge of the GPS monitoring system. The staff involved in the trial received no formal training in relation to the service provider's monitoring system, therefore, it was not possible to articulate the reasons for various inaccuracies or to interrogate the data to decipher what was, at times, displayed by the monitoring software as correct or incorrect. Specific skills and expertise are required with this technology and system to understand the plethora of data that is provided. The existing electronic monitoring programs administrated by QPS and QCS are undertaken by professional staff highly trained in data interpretation.

While the quantitative findings reported in this paper highlight potential problems and inconsistencies regarding the reliability and accuracy of GPS-enabled technology (noting accuracy and reliability of technology constantly evolves), it is also important to note the technology enabled some insight into a person's movements and behavioural patterns that may otherwise have remained unobserved. A number of operational strengths associated with the use of GPS-enabled technology were identified during the trial, including: the increased ability to detect the breaching of a prohibited area given optimal operating conditions, the use of GPS-enabled technology data as a perpetrator accountability tool, and the possibility such data may assist police for intelligence purposes (for example, to place perpetrators in the vicinity of a crime).

A number of complex challenges were also identified by officers during the trial which require consideration. Some are relevant in the event this technology is implemented irrespective of the cohort on which it is imposed, whilst others highlight the limitations of this technology for higher or unpredictable risk cohorts such as perpetrators of DFV. They include technical limitations such as loss of the GPS and cellular signal (both of which are required for GPS-enabled technology to operate), and technical errors such as 'drift' and multipath errors, which impact on the reliability of the data to accurately track the true mapped movements of an individual and subsequently prove genuine breaches. The impact of environmental limitations was also evident as possible causative factors for inaccurate or unreliable GPS data. Finally, functional limitations, including the complexity of the data produced by the monitoring system and faulty equipment limited the effectiveness of GPS-enabled technology to accurately and reliably monitor and track individuals.

GPS-enabled technology was proposed by the Taskforce as one strategy to support victim safety and enhance perpetrator accountability. However, the findings of the technology trial indicate it provides, at best, a moderate level of accuracy and reliability to track an individual's movements and detect the breaching of a prohibited zone, in the absence of a robust case management model supporting the electronic monitoring.

In total, of all the alerts that should have activated, only 49 percent did so, and one in four breaches went wholly undetected, indicating that this technology alone is an insufficient surveillance tool to manage the risk of DFV perpetrators. Consequently, in the event this technology is imposed to assist in the management of DFV perpetrators, at least some breaches will remain unknown and unreported. Based on the findings in this report, it is fair to accept GPS-enabled technology informs as much as it also fails to detect.

The findings demonstrate electronic monitoring alone does not provide a sufficient risk-mitigation solution for high-risk DFV perpetrators and is not an effective or reliable substitute for a robust perpetrator management framework. The findings suggest, it may be an appropriate consideration for lower-risk DFV perpetrators, assuming the risk can be accurately assessed, the technology reliably functions to an optimal standard in the physical location, and if used in conjunction with case management practices to manage the risk posed by a perpetrator released into the community. However, it is also important to note that compliance and attitude towards monitoring on the part of the perpetrator or the victim may further reduce the impact of electronic monitoring.

Therefore, GPS tracking should not be relied on to replace other forms of verification and monitoring, such as contact with police, service providers, a partner, family and other significant third parties. Without a concurrent, clearly structured and sufficiently resourced case management strategy to address the causes of DFV behaviour and the perpetrator's criminogenic needs, GPS-enabled technology is unlikely to provide a risk reduction effect for victims of this crime.

1. Introduction

1.1 Background

In 2015, the Special Taskforce on Domestic and Family Violence in Queensland (the Taskforce), provided its report, *Not Now, Not Ever: Putting an End to Domestic and Family Violence in Queensland* (the Taskforce Report) to the Premier. Recommendation 123 of the Taskforce Report was:

> *The Queensland Government trials the use of GPS monitoring for high risk perpetrators of domestic and family violence*.

The recommendation nominated a trial approach be progressed due to the need to further explore the extent that electronic monitoring is effective in supporting victim safety. The Taskforce also held concerns about the use of electronic monitoring in the domestic and family violence (DFV) context. These concerns include:

- civil liberty and privacy concerns, where victims are required to wear a transmitter;
- unrealistic expectations of victims about the level of safety and security Global Positioning System (GPS) tracking offers;
- the risk that monitoring may be used as a sole alternative to incarceration and, in the absence of other risk mitigation strategies, may reduce security consciousness and reduce protection for victims;
- risks to victims if the technology fails to operate to an acceptable level of capability (given inconsistent satellite and cellular coverage, particularly in regional and remote areas);
- the costs associated with implementing monitoring; and
- over-reliance on technology to mitigate the risks of DFV offending due to the often-unpredictable nature of perpetrator behaviour.

In August 2015, the Queensland Government released its response to the Taskforce Report accepting all the recommendations. In response to Recommendation 123, the Government committed to explore options to monitor perpetrators of DFV, taking into account the full range of potential technological solutions including the use of GPS monitoring, and then trial the most promising model to improve victim safety.[1] In alignment with the technology trial, the Government also committed to commissioning research to explore the electronic monitoring of DFV perpetrators in a range of criminal law contexts – including bail, probation and parole.

Following the Government's response, the *Bail (Domestic Violence) and Another Act Amendment Act 2017* (the Amending Act) was passed to strengthen bail laws. Included in the Amending Act was a provision to allow the court to impose electronic monitoring as a condition of bail for all defendants (not just DFV perpetrators). These changes commenced on 31 March 2018.

The Queensland Police Service (QPS), the Department of Justice and Attorney-General (DJAG), and Queensland Corrective Services (QCS) adopted a joint approach to explore

[1] Reference to 'high risk' perpetrators was omitted in the Government's response to Recommendation 123 as no threshold definition for a 'high risk' DFV perpetrator was provided in the Taskforce's Report. Agencies agree 'high risk' defendants should be managed in a custodial setting.

options for the GPS monitoring of DFV perpetrators. This includes DJAG commissioning external research and the QPS undertaking testing of contemporary GPS-enabled technology in the context of DFV scenarios through a controlled trial. The external research and evaluation of the controlled trial will help the Government to determine if, and when, it may be appropriate to introduce a GPS tracking program for DFV perpetrators to support victim safety. This report is the QPS's key output from the technology trial.

1.2 Overview of electronic monitoring technology

Electronic monitoring is a form of surveillance that can be used to monitor the location and movements of an individual. It is currently employed in over 30 countries and its use varies across all levels of the criminal justice system. The key drivers underpinning the use of this technology are:

- to address prison overcrowding;
- to assist with the high cost associated with keeping offenders in custody;
- to increase offenders' chance of successful reintegration upon release from custody;
- to assist with the case management of an offender under community supervision;
- community concerns about safety and DFV perpetrators; and
- availability and improvements in technology.

The electronic monitoring of defendants and offenders has been operating within Australia for decades. Initially, it commenced via the use of radio frequency (RF) technology in the 1980s as part of a bid to promote community-based sanctions, but it did not build momentum until the early 1990s. RF's popularity was then superseded by GPS technology in the late 1990s.

GPS-enabled technology enables a greater degree of supervision and surveillance due to its ability to geolocate a perpetrator close to real time, as well as detect the breaching of a number of pre-programmed zones that either the perpetrator is prohibited from entering or leaving (see pages 12 and 13 for an explanation of each zone). Due to the numerous tracking functions that GPS-enabled technology offers, all state and territories in Australia that use electronic monitoring have now transferred to primarily using GPS-enabled technology (Bartels and Martinovic, 2017).

To provide greater context to the findings of the QPS technology trial, and noting the complexities associated with the understanding and use of electronic monitoring, a brief explanation regarding the functions of RF and GPS-enabled technology is provided below.

Radio Frequency (RF) Technology

Despite the emergence of GPS technology, RF technology is still used within the criminal justice system in some jurisdictions to verify the presence or absence of an individual within a designated location – typically the individual's residential address under the conditions of home detention or curfew.[2] The technology is programmed to raise an alarm to the related

[2] RF monitoring is used by QCS for some parolees, however, it is used in conjunction with GPS technology, not as a stand-alone monitoring tool. New Zealand continues to use RF technology to monitor defendants and offenders subject to home detention.

monitoring centre in the event the individual exits their restricted area. However, once the individual has departed the area, there is no further capacity of RF to monitor a person and/or track their movements. This type of electronic monitoring is typically only used on low risk offenders due to its limited monitoring scope.

Within a DFV context, RF technology may be utilised for home detention which ordinarily employs unilateral electronic monitoring, with the perpetrator the object of ongoing supervision. However, RF technology has also been adapted for domestic violence situations utilising *bilateral* electronic monitoring (Ibarra and Erez, 2005).

Bilateral electronic monitoring involves a perpetrator wearing a tamper-resistant transmitter on their ankle. A receiver is placed in the home (and/or workplace) of the perpetrator to periodically confirm their presence or absence. A receiver is also placed in the victim's home, synchronised to the perpetrator's transmitter, and will detect the presence of a perpetrator within a range of approximately 150 metres. When a breach of this radius is detected, this should generate an alert to the monitoring centre and law enforcement agencies (Erez, Ibarra and Gur, 2013).

RF technology operates with limited range and capability and relies on a line of sight between the receiver and the tracker. Interference may occur as a result of physical objects (for example, thick walls or several rooms).

Global Positioning System (GPS) technology

GPS-enabled technology improves upon the limitations of RF technology and has several advantages compared to RF. GPS-enabled technology provides information of the individual's whereabouts and monitors where they should and should not be beyond the perimeter of their home or work address.

GPS-enabled technology is designed to track an individual across time and space. It operates on the principle of 'geo-fencing', which entails the programming of multiple and potentially unlimited zones of exclusion (areas an individual cannot go) and inclusion (areas an individual cannot leave).

GPS-enabled technology has largely superseded the use of RF within the criminal justice system due to its versatility, broadened detection range, capacity for multiple zone coverage, and its ability to monitor close to real time the tracked person's whereabouts beyond the immediate range of their home and the person/s they are ordered to stay away from. This is done through the logging of the perpetrator's 'GPS points'.

The increased capacity of GPS technology, however, comes with increased complexities and intricacies regarding its functions. Despite its advantages, the effectiveness of GPS-enabled technology relies on its ability to connect to a satellite signal and a mobile network at the same time and, without this connection, the technology is effectively useless at that time. This connection may be unpredictable and can be interfered with by environmental factors.

a. Access to GPS coverage

GPS tracking technology relies on line-of-sight and connection to a number of satellites. There are between 24 to 32 satellites available to obtain signals from and these GPS satellites are situated approximately 20,000 kilometres from the Earth, known as medium Earth orbits. They take approximately 12 hours to complete an orbit around the

Earth and therefore cross over the same two spots on the equator each day. The angles of the available satellites impact the strength of the GPS signal, with a wide-spread triangulation of satellites (i.e. three or more) providing the best GPS connectivity.

b. Access to mobile coverage

GPS systems also rely on cellular networks to transmit data points related to an individual's location, hence areas with disruptive cellular coverage will impede the ability of the GPS to accurately track the location of the tracked person. Additionally, cellular networks are vital to delivering significant alerts, such as bracelet tampering/removal and/or a breach of an exclusion or separation zone. As a result, ensuring consistent cellular coverage is an important factor.

1.3 Electronic monitoring within a DFV context

In the context of DFV, electronic monitoring is utilised not only to monitor perpetrators, but also, and more importantly, to support victim protection. The underlying rationale for imposing an electronic tracking device on a perpetrator is to deter the individual from approaching or coming into contact with the victim, and to prevent further harm (physical, sexual, or psychological) occurring. To achieve optimal risk mitigation conditions, the location of both the perpetrator and victims should be known with a high degree of accuracy in near real time. Electronic monitoring within a DFV context differs significantly from the typical use of electronic monitoring in that it can involve both the perpetrator and victim subjected to a tracking device to ensure the former is complying with their conditions and the latter's risk to their safety is mitigated. This is referred as bilateral electronic monitoring and it is utilised to offer protection to victims, with their permission and cooperation, rather than focusing on protecting society as a whole.

In the event the perpetrator enters a pre-programmed prohibited zone – be it a geo-fenced exclusion zone or a victim-proximity zone – the technology is designed to detect this and raise an alarm with the monitoring centre affiliated with the program. Similarly, the victim proximity zone is designed to be configured to enable an alert if the perpetrator's anklet device comes within a certain range of the victim's tracking device. The live tracking of both individuals provides an opportunity to reduce police response time for breaches.

Paramount to ensuring an appropriate response following the activation of an alert is the establishment of a dedicated response capability.

Discussion around the development of a model to manage the monitoring of perpetrators of DFV is outside the scope of this report, however, in brief, a 24/7 monitoring service is critical to ensure each alert is immediately interrogated and actioned according to its perceived risk and nature. In addition, immediate availability of a physical field response capability is required to escalate a response in the event the subject does not comply, or does not comply to a satisfactory degree, with the initial directions provided by monitoring centre staff. The field response needs to be informed by a dedicated and standardised response protocol and well-defined procedures are necessary to inform a seamless transition between alert management at the electronic monitoring point and response activity in the field.

Response protocols may vary based on the level of risk posed by a perpetrator. For example, a tiered approach to managing each possible alert may be implemented to effectively balance risk and resourcing requirements, as well as ensure the most appropriate and efficient response is actioned.[3]

A perpetrator's risk profile will similarly inform the intensity of their supervision, as well as the required GPS configuration and alerts necessary to manage their behaviour within the community. For example, a higher-risk DFV perpetrator would require closer supervision by adapting the GPS device to frequently transmit and upload location data to the monitoring system. Conversely, a lower-risk DFV perpetrator may be subject to more passive supervision, with their electronic monitoring data used for retrospective case management and accountability purposes. The rapidly escalating and de-escalating risk profile of DFV perpetrators creates significant practical challenges for monitoring dynamic risk factors to inform supervision and response protocols.

[3] It is not the purpose of this paper to discuss options for implementation of an appropriate field response capability. However, in brief, every possible alert requires assignment of a response category and/or level of priority, with a corresponding action item to be executed by the dedicated response unit. For example, a low-level alert such as notification of a monitored person's battery running low, may be managed by the monitoring centre with a telephone call made to the individual to advise them to recharge their device. For those alerts which have been interrogated and determined by monitoring staff as requiring a more informed investigation, such alerts may be referred to an appropriate field response team, for example the police.

2. Evaluation Purpose and Design

2.1 Purpose

The purpose of this evaluation was to test the reliability and accuracy of GPS-enabled technology within the context of DFV simulated scenarios to inform the Government's considerations of the implementation of this technology for perpetrators of DFV.

2.2 Scope

In scope

The scope of this evaluation will focus only on the practical and operational use of GPS-enabled technology to effectively monitor the movements of a perpetrator of DFV using simulated scenarios, with a key focus on the detection of geographical related breaches.

Out of scope

Outside the scope of this evaluation is a theoretical perspective on the appropriateness and implications of the use of this technology within a DFV context.

2.3 Design

Method

The evaluation method examined in this report is an *outcome* evaluation. It examined the extent to which GPS-enabled technology achieves what it is intended to achieve; that is, to accurately track an individual and activate an alert in the event a pre-programmed zone is breached. The data presented in this report, therefore, provides information specific to these outcome measures.

The methodology underpinning the evaluation is based on a mixed methods approach. It relies on four main data sources:

Quantitative data

- administrative quantitative data extracted from the service provider's monitoring system; and
- manual data recordings of real time and physical location by scenario

Qualitative data

- qualitative data coded from observations by officers conducting the trial; and
- a review of relevant literature analysing the benefits, challenges and limitations regarding the operational use of GPS-enabled technology within a DFV context.

Testing the technology

<u>Equipment</u>

The QPS sourced industry standard, off-the-shelf GPS-enabled electronic monitoring technology required for the trial, including access to a standard electronic monitoring system to enable the monitoring of persons subject to tracking, and alert notification to the monitoring system of all breaches of pre-programmed exclusion, interest and victim-proximity zones (see below for a description of each of these zones).

In conjunction with the monitoring software system, the following equipment was provided for the technology trial:

- The electronic monitoring device attached to the subject's ankle which allows the person (i.e. the DFV perpetrator) to be tracked by the monitoring system. A key feature of the device is its ability to generate pre-programmed alerts, for example, when the conditions of an exclusion or interest zone are breached.
- Victim tracking devices that may be carried by the DFV victim (with their consent and cooperation) and enables them to be tracked to support their safety. This device generates alerts when the perpetrator breaches a victim-proximity zone.
- Separate victim-carried device which enables the victim to generate a 'call to help' alert to the monitoring system with a GPS location, as well enabling a two-way voice communication to a specific dedicated pre-programmed telephone number.
- RF beacon powered through a normal 240V power outlet at the perpetrator's and/or victim's residence and/or workplace. It prolongs the battery life of the perpetrator's device and is used in places where the GPS signal is insufficiently reliable. It provides a more accurate ability to locate a monitored person but within a much smaller geo-fenced area. For the purposes of this trial, the RF beacon was used to assist the detection of a breach of an exclusion zone.

<u>Location</u>

Locations across Queensland were selected to test the GPS-enabled technology in different environmental conditions characterised by variable geographical features which may influence the technology's ability to accurately and reliably track and locate perpetrators of DFV. Whilst it is not possible to conclude that any inaccuracies found during this trial are directly related to an area's topography, the findings may provide further insight into the operational deployment of this technology in certain settings.

<u>Scenarios</u>

Testing the technology using simulated scenarios, as opposed to establishing a live trial, was the preferred methodology to progress the Taskforce's recommendation *to trial the use of GPS monitoring for high risk perpetrators of DFV*.

The use of this technology within a DFV context is still a relatively new concept in Australia and there are a number of concerns regarding its use for DFV perpetrators. This is due to the largely unpredictable and highly emotional nature of DFV crime. Furthermore, no evaluation has been undertaken to date by any Australian jurisdiction regarding the reliability of GPS monitoring, therefore questions remain regarding the effectiveness of this technology to accurately track and monitor individuals.

Expert advice was obtained to support the creation of DFV scenarios to trial. Seven scenarios were created and trialled in each location to assess the effectiveness of the technology. The scenarios involved simulating real-world environments, including a perpetrator approaching a victim's residence or workplace and chance encounters in unregulated public places. A perpetrator subject to electronic monitoring will usually have conditions imposed (e.g. they are not permitted within 100 metres of the victims' residence or workplace) and so specific distances were applied for each zone examined as part of the trial.

Three QPS officers were involved in the enactment of each scenario: one posed as the perpetrator and wore the GPS tracker; the second posed as the victim; and the third gathered administrative data to record real time and physical location information based on the perpetrator's movements and breach actions.

<u>Alerts</u>

Prohibited zones are mapped by a series of geometric points around a location and recorded within the monitoring system. An alert occurs when a tracked person's location is found to be within this geo-mapped prohibited area.

The GPS-enabled technology allows for geographical related conditions to be imposed, therefore, if a perpetrator enters within a prescribed distance of a location, this should generate an alert in the monitoring system to notify a breach occurring. Monitoring staff can attempt to intervene directly with the subject to verbally direct them to relocate or forward the alert to the appropriate authorities for an actioned response.

The scenarios involved QPS staff members purposely breaching conditions (or, in the case of one scenario, purposely avoiding breaching the conditions) to determine the efficacy and responsiveness of the technology to generate the appropriate alerts in the monitoring system. Whilst there are numerous alerts that can be pre-set into the monitoring system, the following alerts were pre-programmed for activation during this trial.

Exclusion zone (GPS)

An exclusion zone alert occurs when a monitored person enters a pre-set geographically fenced area which they have been ordered not to enter (for example, a victim's residence or workplace). Varying distances can be pre-programmed within the system to nominate the size of the exclusion zone.

Exclusion zone (RF beacon)

This alert occurs when a monitored person enters a pre-set location which has a RF beacon installed and which the person has been ordered not to enter. The system can pre-set the size of the zone, though is limited to a smaller range than the GPS exclusion zone due to the lesser capability of RF. Maximum coverage is limited. This zone is used at locations where GPS data may be unreliable or infrequent.

Interest zone - Exclusion (GPS)

An interest zone alert will activate when the monitored person enters a pre-set geographically fenced area. The purpose of an interest zone is to provide the monitoring centre with a warning that the perpetrator is heading in the direction of the victim, albeit no breach has yet occurred. This type of zone essentially acts as a buffer and may assist in understanding the patterns of a perpetrators' behaviour, particularly if there is some indication the perpetrator is scoping the perimeter in wait of the victim.

Victim Proximity

A victim proximity alert is generated when the perpetrator approaches and breaches a pre-set separation area between themselves and the victim. This alert is based on GPS signal to determine any breaches of proximity. This alert is specific to a victim device.

The table below provides a brief description of each scenario and the alerts that were pre-programmed for generation to test the reliability and accuracy of the technology.

Table 1: Scenario by tracking device

Scenario	**Perpetrator wearing a tracker**	**Victim has a tracker**	**RF beacon**
1. Perpetrator approaches the residence of the victim with an exclusion zone imposed. Pre-programmed alert: Exclusion zone GPS	Yes	No	NA
2. Perpetrator approaches a static location with an exclusion zone imposed. Pre-programmed alerts: Exclusion zone GPS, Exclusion zone RF, Victim proximity zone, Duress alarm.	Yes	Yes	Fixed
3. Perpetrator approaches a mobile victim with an exclusion zone imposed. Pre-programmed alerts: Exclusion zone RF, Victim proximity zone	Yes	Yes	NA
4. and 5. Chance meeting – Perpetrator approaches victim within an unregulated public place. Pre-programmed alerts: Victim proximity device	Yes	Yes	NA
6. Perpetrator is aware of the victim location and exclusion zone and moves into close proximity without breaching the exclusion zone. Pre-programmed alert: None	Yes	No	NA
7. Perpetrator is aware of geo-fenced location and exclusion zone and moves into close proximity without breaching the exclusion zone. Pre-programmed alert: Interest zone GPS	Yes	No	Fixed

3. Findings

The findings reported below are based on seven DFV simulated scenarios across various locations chosen to test the accuracy and reliability of GPS technology.

In total, 35 scenarios were carried out and just over half (51 percent) were found to be a complete success – that is, each alert activated as required according to the pre-programmed conditions of the scenario.

An additional 23 percent were found to be partially successful, meaning at least one alert, from a possible two, three, or four alerts, activated following the breach of a zone.

Finally, 26 percent of scenarios failed, meaning no alert/s activated following the breaching of a zone. Put more simply, one in four breaches occurred with no breach notification alarm at all and therefore occurred wholly undetected.

3.1 Reliability

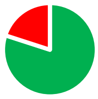
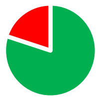
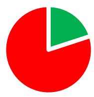
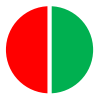
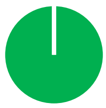
Alert reliability by tracking device

As identified in Table 2, each scenario was configured to generate one or more alerts depending on which tracking devices were included for testing purposes. For example, scenario one was based on a simple unilateral design, involving only the perpetrator device, and so only one alert was pre-programmed for activation following the breaching of the exclusion zone. Scenario two, on the other hand, was based on a bilateral design and included the perpetrator device, the victim-proximity devices, as well as the RF beacon. Subsequently, each device should have activated an alert once the exclusion zone was breached.

There were significant differences in the reliability of each device to detect a breach and trigger an alert to the monitoring system. The perpetrator device did not always accurately detect and activate an alert when the perpetrator entered a smaller exclusion zone but was always accurate when the perpetrator entered an interest zone. The RF beacon detected the breaching of an exclusion zone more often than not.

The victim tracking devices, on the other hand, were largely unreliable in terms of detecting the perpetrator breaching a pre-set proximity distance between the two devices, with the devices activating an alert only 35 percent to 38 percent of the time.

Table 2: Reliability of tracking device to detect a breach and activate an alert

Scenario	Exclusion zone alert		Interest zone alert	Victim-proximity zone alert	
	GPS	RF	GPS	Tracking Device only	Tracking and Duress Alarm Device
Scenario 1					
Scenario 2					
Scenario 3					
Scenario 4					
Scenario 5					
Scenario 6					
Scenario 7					
Total	6/10 alerts activated (60%)	6/10 alerts activated (60%)	5/5 alerts activated (100%)	7/20 alerts activated (35%)	6/16 alerts activated (37.5%)

Green = Alert received Red = Alert not received

Time lag

A time lag refers to the time between an action which should trigger an alert and the time when the monitoring system registers the alert. To remove any doubt, a time lag in no way implies a physical response to an alarm raised by the monitoring system.

Based on the technology used in this trial, there is an inevitable short time lag between an individual's real time physical movements, and that which is communicated to the monitoring system. Subsequently, in the event an alert is generated, the alert notification dispatched by the monitoring centre occurs shortly after the relevant breach.

3.2 Accuracy

For GPS-enabled technology to detect an exclusion or interest zone breach, it requires the ability to accurately obtain, track and record the geographical movements and location of the perpetrator, whilst detection of a separation zone breach is contingent upon its effectiveness to obtain, track and record the location of both a victim and perpetrator.

It is also important to note that the level of tracking detail provided in a map is informed by the pre-programmed rate of location 'pings'. The ping rate is a term used to describe the time set between recording and uploading the geographical location of a device. This function will vary based on the assessed risk of the individual being monitored and the underlying reason for tracking their movements. For example, high risk offenders require continuous active surveillance, whilst low risk offenders may be monitored more so for retrospective case management and accountability purposes. The intensity of monitoring will depend on the individual's risk profile and this will inform how frequently an individual's geo-graphical location is uploaded. For example, high risk offenders may have their geo-graphical location set to be uploaded every five to ten seconds, whilst for a low-risk offender, this may be programmed at ten-minute intervals.

For the purposes of this evaluation, the perpetrator's geo-graphical location was set for detection at 30 second intervals to enable a detailed analysis of the accuracy of the system's mapping capabilities. Accuracy appeared to vary depending on the physical environment and topographical features, with discrepancies of up to 150 metres between the subject's actual position and location reported through the monitoring software recorded in some locations. In other locations, the discrepancy was reduced to no more than a few metres, which, while falling short of a forensic evidentiary standard, could meet operational tolerances.

Although the quantitative findings identified potential problems and inconsistencies regarding the reliability and accuracy of GPS technology, it is also important to note that this technology provides insight into a person's movements and behavioural patterns that is otherwise unable to be detected in the absence of this technology. A number of operational strengths associated with the use of GPS-enabled technology were identified during the trial that may improve the way perpetrators of DFV are monitored in the community.

Detection of breaching prohibited areas that previously may have gone undetected

GPS-enabled monitoring provides a degree of supervision and surveillance that is otherwise unobtainable. Despite findings showing that only half of all pre-programmed alerts activated when a prohibited zone was breached, it is reasonable to conclude that such breaches would have otherwise gone undetected unless witnessed by a person aware of the restricted boundary (for example, the victim). During the trial, the GPS-enabled technology provided close to real time data when an alert activated (on average, a delay of two to three minutes) and a reasonable indication of the perpetrator's presence in the vicinity. In the event these scenarios were live, law enforcement agencies would have received notification of a breach within a few minutes of its occurrence and therefore would have been able to respond more efficiently and effectively.

GPS-enabled technology will enable the detection of more geographical related breaches, not because more are occurring, but because of the capabilities of the technology. Furthermore, assuming the individual's state of mind promotes rational and objective decision making, the knowledge that their geographical movements are being tracked may operate to deter some perpetrators from contravening such conditions (and ultimately, deter them from approaching the victim).

Accountability

GPS-enabled technology enables another layer of accountability for the perpetrator as it provides retrospective data of their whereabouts and monitors where they are permitted and not permitted to be. It may also be used to identify sinister behavioural patterns amongst those DFV perpetrators motivated to breach the conditions of any order imposed on them. It is likely that such perpetrators might use the GPS tracking technology to further manipulate and antagonise the victim by entering the interest zone but remain outside the exclusion zone (and therefore technically not breaching the order). The electronic monitoring system enables interrogation of behavioural patterns such as evidence of stalking behaviour, to enable the perpetrator to be held accountable for behaviours that previously would have gone undetected.

3.3 Limitations within a DFV Context

The technology trial highlighted complex challenges and issues regarding the reliability and accuracy of GPS-enabled technology that are particularly pertinent if this technology is to be implemented in a DFV context where there is a need for an agile victim proximity model which requires constant adjustment as they move about the community. They include technical, operational and functional limitations and all have a significant impact on the feasibility and practicality of implementing this technology to track and monitor DFV perpetrators as a stand -alone risk mitigation approach.

Technical limitations

Possibly the most significant limitation of this technology, and one which is particularly important within a DFV context, is the inability to rely on the technology to consistently operate at optimal capability. The findings from the trial demonstrate the possibility GPS connectivity is occasionally intermittent, and so reliability is never absolute.

For GPS monitoring to be effective, there must be access to GPS coverage (i.e. satellites) to establish location and the device must be within an area serviced by a mobile network in order for location information to be reported to the monitoring service. When network access is unavailable, the device will not be able to communicate the location of a perpetrator or victim to the monitoring service until the connection is reactivated. Without GPS connectivity, the ability to retrospectively track the true physical movements of an individual are lost, with pre- and post-signal points treated just as any other two points and connected with a straight line.[4] Instances involving lost GPS and mobile network signal occurred frequently during the trial, particularly in certain areas.

Drift

Drift occurs when the location points specified on the monitoring map are inaccurate, thus displaying either incorrect position readings or no readings at all. These position errors occur because GPS receivers require an unobstructed view of the sky and therefore experience technical limitations when inside buildings, underwater or underground. Due to approximately 32 GPS satellites continuously moving and the propagations of radio signals in the air being affected by many factors, including weather, environmental factors or building structures, a slight deviation can cause errors in recorded location data ranging from metres to several kilometres.

The implications of drift are significant and will impact the feasibility of relying on this data to accurately determine a perpetrator's true movements, which will consequently impact the confidence that victims and police have in the technology. For example, drift may cause 'false alerts' to occur, whereby the system generates an alert when in fact no breach actually occurred. Such technical faults result in difficulties proving genuine breaches and enables the reliability of the equipment to be challenged in court. It may also subject perpetrators to breach-related proceedings based on inaccurate readings when in fact, there was no breach. Furthermore, it may result in cynicism amongst officers regarding the operation of the technology and consequently impact on prioritising responses to breach notifications. Police having to respond to false alerts also creates additional risk when urgently ('lights and sirens') responding to an alert, generates an unnecessary time impost on frontline policing resources establish whether an alert was in fact false, and creates risks to victims if police inadvertently consider a real alert to be false. Finally, such technical failures create a greater workload for the monitoring staff and require them to interrogate circumstances that are null and void.

Ping rate set high > 30 seconds

The ping rate is a term used to describe the time set between recording the geographical location of a device. It is understood that the standard set rate is 30 seconds, though this appears to be a rough setting which varies at times to more than this set time. Increasing the rate to more than 30 seconds does save the battery life of the device, but this does not provide an accurate route travelled by the tracked person, particularly when the individual is travelling via a motor vehicle. The system joins the recorded dots (locations), to show a

[4] For example, in May 2018, Telstra experienced an outage which caused electronic monitoring devices to fail in the Northern Territory, South Australia and Queensland, resulting in over 800 offenders across all three jurisdictions unable to be monitored for several hours. The devices automatically reconnected when the network was restored (Sveen, 2018).

direction of travel. When the ping rate is increased to longer periods between each ping, the 'dots' that represent each ping are further apart and joined by a straight line instead of the variations between pings. This results in an incorrect visual indication of any true route taken.

A challenge with a 30 second ping rate (or greater than a 30 second ping rate) is that it enables a tracked person to enter and then leave an exclusion zone or leave and re-enter an inclusion zone within this 30 second window without an alert being generated. This occurred during one scenario when the perpetrator was able to breach the zone twice before finally generating an alert. This risk might be managed operationally by setting large exclusion zones that would take longer than 30 seconds to enter and exit. Of relevance is that generally individuals subject to electronic monitoring do not know the exact parameters of the exclusion zone.

Environmental issues

Geography is another important dynamic that was shown to impact the effectiveness of GPS-enabled technology to track and monitor an individual's movements.

Different geographical areas have varying cellular coverage; hence the accuracy and reliability of GPS systems can be more limited in areas with spotty cellular coverage (Waldo, 2014). Added to this, cellular connectivity is likely to be adversely affected if the individual being tracked is in a high network demand area resulting in lost or intermittent connectivity.

The above limitations do not only adversely impact the effectiveness of GPS-enabled technology to accurately and reliably track an individual imposed with a tracking device, but they also create technical problems and result in negative outcomes such as 'false alerts' and 'drift effect'.

Functional limitations

Complexity of data and system

An important finding of the GPS-enabled technology trial, and which was a significant obstacle experienced by the QPS staff involved in the technology trial, was the complexity of the tracking data that was captured and recorded on the monitoring system for interpretation purposes.

GPS-enabled technology provides a great deal of information, however, understanding and interpreting this data requires specialised skills and an in-depth knowledge of the GPS monitoring system. Consequently, GPS tracking creates greater workloads on staff owing to a more complex and extensive information stream, which could impact on the ability of staff to effectively supervise individuals subject to a tracking device.

The staff involved in the trial received no formal training in relation to the service provider's monitoring system, therefore, it was not possible to articulate the reasons for various inaccuracies or to interrogate the data to decipher what was, at times, factually correct or incorrect. Specific skills and expertise are required with this technology and system to understand the plethora of data that is provided.

Faulty equipment

Prior to commencing the trial, preliminary tests were undertaken to acquaint the participants with the system and equipment. It was during this pilot test that one of the perpetrator devices was identified as possibly malfunctioning and was discontinued from inclusion in the trial. A second device appeared to be functioning correctly and was included in the trial. This finding raises the possibility that some individuals issued with this technology may be subject to a faulty device, despite prior clearance regarding its use from the service provider.

Another issue identified in relation to the functionality of the tracking devices was the variable performance of the two victim proximity tracking devices to accurately track and generate an alert in the event a victim proximity zone was breached. This is despite both devices being carried by the same participant in the same manner throughout each scenario, with minimal distance apart throughout. It was regularly found that one device would record geographical locations, whilst the other failed to do so. This resulted in the former device failing to generate a victim proximity alert.

A well-founded GPS-enabled electronic monitoring program would need comprehensive and validated configuration and testing protocols to address the implications of defective equipment.

4. Reflections and Conclusions

With electronic monitoring proposed by the Taskforce as one strategy to improve victim safety and augment perpetrator accountability, the findings of the technology trial indicate it provides, at best, a moderate level of accuracy and reliability to track an individual's movements and detect the breaching of a zone in the absence of a robust case management and surveillance framework and supported by staff appropriately trained in data interpretation.

As shown, one in four breaches occurred with no alert generated by the tracking device/s utilised for the scenario, indicating that this technology alone is not an effective surveillance tool to manage the risk of DFV perpetrators breaching prohibited zones. Furthermore, a total of 49 percent of all tracking device alerts triggered when they should, demonstrating that as many alerts are generated as are not.

The victim tracking devices were particularly unreliable in detecting the approaching proximity of the perpetrator, with an average of two in three non-detections. In the event this technology is implemented live for DFV perpetrators and victims, the findings highlight concerns that many breaches may occur with no corresponding system notification. Conversely, and as outlined in the technical limitations regarding this technology, there is also the potential to create false and misleading information which may have unintended consequences and lead to unjust outcomes for perpetrators in cases where the GPS-enabled technology registers false alerts due to the lack of accuracy.

The objective of this trial was based on the operational capabilities of GPS-enabled technology, particularly in relation to how reliably and accurately this technology performs when utilised in a DFV context. It was assessed solely as a stand-alone risk management strategy.

It is important to note the imposition of GPS-enabled technology within the criminal justice system is, for the most part, situated as an additional risk management tool in conjunction with a wider, individualised case management framework. For example, GPS-enabled technology has been used by QCS for almost eight years for monitoring serious sex offenders subject to continuing supervision orders under the *Dangerous Prisoners (Sexual Offenders) Act 2003* (DPSOA) and, more recently, for offenders released on parole. However, for these offender cohorts, QCS utilises GPS-enabled electronic monitoring as a tool to support a robust multi-faceted case management and surveillance model. It is not relied upon as the primary risk mitigation tool in high or imminent risk situations. It assists in identifying patterns of behaviour and non-compliance. The decision to apply GPS monitoring is guided by an individualised assessment of an offender's risks and circumstances, the technical performance of the equipment at the location/ s frequented by the subject, and the benefits that could be derived using such monitoring alongside consideration of the available operational response capability. QCS conducts assessments on the offenders' homes and communities to determine whether GPS monitoring will function in those locations or whether there are telecommunication limitations that may impair the electronic monitoring functionality. There are also clear management options for these offenders, including return to prison for non-compliance or increased risk.

For GPS-enabled technology to be of use within the DFV space, policies and practices guiding the use of the technology must be shaped according to strategic goals and consideration of its limitations. For example, to provide an additional risk mitigation tool to monitor perpetrator movements for accountability purposes, not as a stand-alone life-saving protection tool. A DFV GPS-enabled technology model should be based on an understanding of the dynamics of DFV, rather than utilising this technology to achieve broader criminal justice challenges and objects (for example, prison over-crowding, remand reduction, court backlogs). Understanding these dynamics, and the risks they pose to the victim, especially during critical phases (e.g. post-assault, separation), could enhance the effectiveness of this technology to deter contact between the perpetrator and victim.

Balancing the benefits, limitations and unintended consequences of GPS technology, the findings demonstrate electronic monitoring does not provide an effective risk-mitigating solution for high-risk DFV perpetrators and is not a reliable substitute for perpetrator case management.

The trial suggests it may be appropriate for consideration for lower-risk DFV perpetrators if used in conjunction with case management practices to manage the risk posed by a perpetrator released to the community.

Furthermore, it should not be relied on to replace other forms of verification and monitoring, such as contact with police, service providers, partner, family and other significant third parties. Without a concurrent case management strategy to address the causes of DFV behaviour and criminogenic needs, GPS-enabled technology is unlikely to provide a risk reduction effect.

Underlying the need for a wider case management strategy is a dedicated team to manage and support perpetrators subject to GPS-enabled monitoring, similar to the case management plans implemented by QCS for serious sex offenders who require ongoing surveillance and monitoring. This would provide the individual with a central point of contact, enhance the supervision of the perpetrator imposed with this technology, improve their rehabilitative and reintegration prospects, and ultimately strengthen an agency's ability to safely manage perpetrators in a community setting. Added to this, GPS-enabled technology provides a great deal of information, however, understanding and interpreting this data requires specialised skills and in-depth knowledge of the GPS system. Subsequently, adequately qualified staff are vital to ensure the information is interpreted and interrogated accurately.

Beyond its use as an additional risk management tool for perpetrators (and possibly victims) of DFV, the findings presented regarding the reliability and accuracy of GPS-enabled technology present challenges in relation to the admissibility of the system's data in a criminal justice context. For example, technical limitations (e.g. multipath errors, drift, false alerts) may provide be used to contest authenticity of the data in court.

Another important consideration regarding the capabilities of GPS-enabled technology that is particularly important within a DFV context, and which is contrary to public expectation, is the inability of GPS-enabled technology to provide real time monitoring.

Based on the technology used in this trial, there is an inevitable time lag between an individual's real time physical movements, and that which is communicated to the monitoring system. Subsequently, in the event an alert is generated, the alert notification dispatched by the monitoring centre to the appropriate authority does not occur as soon as a breach occurs, but rather, in a best-case scenario, a few minutes following the occurrence of the relevant breach. Consequently, GPS-enabled technology should not be considered as an emergency intervention tool. Added to this, GPS-enabled technology does not have intrinsic supervisory powers. It provides an indication of a person's location but reveals nothing about what they are doing and in the event a perpetrator decides they will commit further offences against their victim, this technology will not prevent this.

To conclude, the outcomes of this trial demonstrate this technology may benefit individuals affected by DFV by increasing perpetrator accountability, deterring perpetrators from approaching the victim, enabling retrospective monitoring, and finally assist police to prove offences that centre on proximity or contact conditions, but to what extent is unknown given the possible challenges of the admissibility of GPS-enabled technology as evidence.

5. Bibliography

Bartels, L., & Martinovic, M. (2017). Electronic monitoring: The Australian experience, *European Journal of Probation*, Vol 9(1): 80 – 102.

Bales, W.D., Mann, K., Blomberg, T., Gaes, G., Barrick, K., Dhungana, K., and McManus, B. 'A Quantitative and Qualitative Assessment of Electronic Monitoring' (May 2010) Report prepared for the US Department of Justice.

DeMichele, M. (2014). Electronic monitoring: It is a tool, not a silver bullet, *Criminology and Public Policy*, 13(3): 1 – 8.

Erez, E., Ibarra P.R., and Gur, O.M. (2013). Using GPS in Domestic Violence Cases: Lessons from a Study of Pretrial Programs, *Journal of Perpetrator Monitoring* Vol 5.

Erez, E., Ibarra, P.R., Bales, W.D., and Gur, O.M. (2012). GPS Monitoring Technologies and Domestic Violence: An Evaluation Study. Report prepared for the US Department of Justice.

Gable, R., and Gable, K. (2007). The Practical Limitation and Positive Potential of Electronic Monitoring, *Corrections Compendium* Vol 32(5), 6.

Ibarra, P.R., and Erez, E. (2005). Victim-centric Diversion: The Electronic Monitoring of Domestic Violence Cases, *Behavioural Sciences and the Law* Vol. 23, 259.

Nellis, M. (2010). Electronic monitoring of perpetrators. In Herzog-Evans, M (ed.), *Transnational Criminology Manual*. Oisterwijk: Wolf Legal Publishers, pp. 391 – 410.

Scottish Government (2013). *Development of Electronic Monitoring in Scotland: A Consultation on the Future Direction of the Electronic Monitoring Service*. Edinburgh: Scottish Government.

Sveen, B. (2018). Telstra outage causes prisoners' tracking devices to fail. *The New Daily*.

Waldo, J. (2014). Implementing a GPS Tracking Program for Community-based Perpetrators: What Correctional Agencies Need to Know, *Journal of Perpetrator Monitoring*, Vol 16.