



# **Debugging Hardware and Family Violence: A Market, Technical, and Legal Analysis**

*Technology-Facilitated Family Violence Research Group*

**Deakin University**

**Dr Diarmaid Harkin, Faculty of Arts and Education**

**Dr Samer Hanoun, Institute of Intelligent Systems Research  
and Innovation**

**Associate Professor Marilyn McMahon, Faculty of Business**

## EXECUTIVE SUMMARY

### Debugging Hardware and Family Violence: A Market, Technical, and Legal Analysis

Between November 2017 and March 2018, the *Technology-Facilitated Family Violence Research Group* undertook a small-scale study into the use of physical ‘debugging’ hardware in the context of family violence. The study comprised three key elements: a market analysis of the range of commercially-available physical debugging equipment in Australia; a technical analysis of a small sample of ‘debugging’ devices; and an analysis of the legal framework in Victoria governing surveillance and the discovery of malicious ‘bugs’.

The key findings of this study are:

- **Market Analysis:** A number of radio frequency (RF) detectors are sold as ‘bug detectors’ in Australia. The prices range from devices that can be secured for \$100 or less, a larger number of devices that are within the \$100 to \$1000 range, and then a range of devices over \$1000. It is possible to purchase devices with price tags exceeding \$6000. It is unclear from the advertising claims of ‘bug detectors’ whether they are suitable to be used for countering malicious surveillance in the context of family violence.
- **Technical Analysis:** A sample of five devices, ranging from cost value of \$29.95 to \$1454.34 were purchased and tested under laboratory conditions. The devices were tested against their ability to detect RF signals from equipment such as a Wi-Fi router, a phone operating on 3G, a phone operating on 4G, a laptop with Bluetooth enabled, and a RF signal-generator transmitting at 1GHz. These equipment are used to simulate similar transmission signals of real ‘bugs’.
  - o Devices were tested against a number of criteria including their detection range, accuracy, sensitivity of detection, nature of feedback, ease of use, calibration requirements, clarity of instructions, and other criteria.
  - o More expensive equipment performed better at detection with greater detection distances, but some devices were significantly higher in price without significant increase in accuracy.
- **Legal Analysis:** A number of criminal law cases and family law cases have appeared before the courts in Victoria involving technology-facilitated stalking and surveillance.
  - o A range of laws were identified that can be used to regulate stalking and surveillance (including the use of ‘bugs’) in the context of family violence. They include stalking laws (*Crimes Act 1958 (Vic) s 21A; Personal Safety Intervention Orders Act 2010 (Vic); Family Violence Intervention Orders (Vic)*); surveillance laws (*Surveillance Devices Act 1999 (Vic)*); Commonwealth laws concerning communications (*Criminal Code Act 1995 (Cth); Telecommunications (Interception and Access) Act 1979 (Cth)*); recklessly putting others at risk of death or serious injury (*Crimes Act 1958 (Vic) ss 22, 23.*); and new laws relating to the use of intimate images (*Summary Offences Act 1966 (Vic)*).
  - o The analysis identified the importance of obtaining and retaining evidence of technology facilitated family violence so that it can be used in criminal prosecutions. For instance, when a ‘bug’, is discovered, photographic records of the device ‘in situ’ should be created.

## CONTENTS

<b>EXECUTIVE SUMMARY</b>	<b>Page 2</b>
<b>BACKGROUND AND RESEARCH QUESTIONS</b>	<b>Page 4</b>
<b>PART 1: MARKET ANALYSIS</b>	
Part 1 (i): Outlining the market analysis	Page 5
Part 1 (ii) Conclusion of market analysis	Page 7
<b>PART 2: TECHNICAL ANALYSIS</b>	
Part 2 (i): A note on bugging devices and RF detectors	Page 8
Part 2 (ii): The sample	Page 9
Part 2 (iii) Testing the devices	Page 10
Part 2 (iv) The results	Page 11
Part 2 (iv) Conclusion of technical analysis	Page 16
<b>PART 3: LEGAL ANALYSIS</b>	
Part 3 (i): Surveillance, bugs and legal definitions of family violence	Page 17
Part 3 (ii): The prevalence of technology-facilitated family violence and abuse	Page 17
Part 3 (iii): The legal regulation of technology-facilitated family violence and abuse in Victoria	Page 18
Part 3 (iv): Evidence gathering for criminal prosecutions	Page 20
Part 3 (v): Conclusion	Page 20

## BACKGROUND AND RESEARCH QUESTIONS

### Background to the research

The Victorian Government's newly-established *Family Safety Victoria* is implementing a number of programs to prevent family violence. One program, the *Personal Safety Initiative (PSI)*, seeks to use private security companies and technology to support victims of family violence. The PSI will implement the use of private security and technology across the state's 18 RAMPs (Risk Assessment and Management Panels).

The Senior Project Officer and state-wide coordinator of the PSI, Ms Kate Ball, has identified a specific need for *Family Safety Victoria* to develop more knowledge of physical debugging equipment. There is an increasing prevalence of perpetrators of family violence using bugs, cameras, physical tracking devices and mobile phones surreptitiously planted around the home, car or workplace of victims. The PSI wishes to combat this development and support family violence services to 'debug' the homes of victims.

Following conversations with Dr Diarmaid Harkin, Ms Ball sought the advice of *The Technology-Facilitated Family Violence Research Group* at Deakin University. The goal of Ms Ball was to orientate *Family Safety Victoria* to the capabilities and market for counter-surveillance bug-detection hardware. *Family Safety Victoria* faced the following key challenges:

- They have little knowledge of the current market for bug-detection hardware
- They have little technical knowledge of the capabilities of bug-detection hardware
- They have little sense of what is value-for-money in the market and what are the reasonable costs for equipment that can detect signals from tracking devices, cameras, mobile phones and other 'bugs'
- They are uncertain as to the legal ramifications when a 'positive' discovery of malicious surveillance is discovered

To that end, the *Technology-Facilitated Family Violence Research Group* at Deakin University accepted a request to support *Family Safety Victoria* in addressing these challenges. The research was jointly-funded by a number of departments at Deakin University including the Faculty of Arts and Education, the Institute for Intelligent Systems Research and Innovation (IISRI) and the Faculty of Business and Law. The research budget was \$9000 in total. The size, scale, depth and conclusions of the project should be considered in relation to this relatively modest budget.

Between October 2017 and March 2018 *The Technology-Facilitated Family Violence Research Group* conducted research to address the following three primary research questions:

Principal Research Questions	Research Methodology
<i>What is the range of physical debugging equipment available on the market today?</i>	(a) A market analysis of bug detection hardware that is available in Australia.
<i>What are the capabilities of physical debugging equipment?</i>	(b) A technical analysis of a select sample of devices identified within the market analysis stage.
<i>What are the legal implications when a 'bug' is discovered?</i>	(c) A legal analysis of the implications for family violence services when they uncover a 'positive' test for bugs in the context of searching for surveillance in the homes of victims.

## PART 1: MARKET ANALYSIS

### Part 1 (i): Outlining the market analysis

The first stage of research was market analysis. Conducted primarily by Dr Diarmaid Harkin (Faculty of Arts and Education, Deakin University), the goal was to catalogue vendors of debugging equipment within Australia and scope the range of devices that are commercially available for purchase. The market analysis concluded with a sampling decision of a select number of devices to be tested within the technical analysis.



Using a number of keyword searches, Dr Harkin identified nine prominent vendors of bug detection hardware within Australia.



From analysing the catalogue of bug detection hardware sold by the vendors highlighted above, five distinct bands of price category were identified:




- Category A - Under \$100
- Category B - \$100 to \$400
- Category C - \$400 to \$1000
- Category D - \$1000 to \$2500
- Category E - \$2500 to \$9000

See below for an example of the type of device that falls within each category band and the advertising claims made in respect to each product:

Category	Name of Example Device	Picture	Advertising Claims	Price
Category A – Under \$100	Compact Camera and Bud Detector		Frequency Range: 1.0Mhz-6.5Ghz Telephone Tap Detection Hidden Camera Detection Mobile Phone Detection For Detection of Wired Camera Lenses For Detection of Wireless Camera Signal and Lens For Detection of RF Bug Frequencies  (Source: OzSpy <sup>1</sup> )	\$99.95
Category B - \$100 to \$400	Protect 1203 Portable Spy Bugs Found Detector		Frequency range 30—6000 MHz  (Source: SecurityLab <sup>2</sup> )	\$295.00

<sup>1</sup> <https://www.ozspy.com.au/surveillance-equipment/spy-equipment/bug-detection-and-camera-detection/camera-detector>

<sup>2</sup> [http://www.securitylab.com.au/professional-spy-phone-bugs-found-detector-protect-1203.html?filter\\_name=Protect%201203](http://www.securitylab.com.au/professional-spy-phone-bugs-found-detector-protect-1203.html?filter_name=Protect%201203)

<p><b>Category C - \$400 to \$1000</b></p>	<p><i>Pro01 Professional Bug Detector</i></p>		<p>Frequency range: 1 MHz - 6 GHz “Detects all s of FM, VHF and UHF listening devices as well as all 1.2, 2.4 and 5.6 GHz wireless hidden cameras. The Pro01 radio frequency tracer is useful in locating stuck transmitters or bugging devices in a room or automobile. It excels at silent detecting RF signals for RF security and counter-surveillance applications.”</p> <p>(Source: EyeSpyWorld<sup>3</sup>)</p>	<p>\$585.00</p>
<p><b>Category D - \$1000 to \$2500</b></p>	<p><i>RFDS-5 25GHz Transmitter Finder</i></p>		<p>High frequency range (detection up to 25GHz)  “Professional bug detector. Detects all FM, VHF and UHF listening devices as well as all 1.2, 2.4 and 5.6 GHz wireless hidden cameras”  “Detecting all radio devices including digital encoded  Detecting spread spectrum, hopping and pulse transmissions  Detecting mobile phones and computers (including manipulated devices)”</p> <p>(Source: Hidden Camera Surveillance<sup>4</sup>)</p>	<p>\$1677.27</p>
<p><b>Category E - \$2500 to \$9000</b></p>	<p><i>CAM – 105W Mobile Phone Detector</i></p>		<p>“The CAM-105w Cellular Activity Monitor is a handheld multiband cellular signal detector ready for the latest generation of 4G devices (as well as existing 2G and 3G), plus Wi-Fi/Bluetooth devices.</p> <p>The CAM-105w is designed to detect and locate transmissions from cellular mobile phone based devices including mobile phones, PDAs and smartphones, vehicle trackers, GSM listening devices (bugs) and covert wireless 3G/4G cameras.”</p> <p>“Detects GSM (2G), UMTS (3G), 4G (LTE) - plus Wi-Fi/Bluetooth/2.4 Ghz devices  Detects Mobile Phones, Smartphones, GPS Trackers, SMS (Texts), 3G/4G Video, Bluetooth &amp; Wi-Fi Devices  Detects Cellular Bands 800 MHz (4G), 900 MHz (2G), 1800 MHz (2G/4G), 2100 MHz (3G), 2600MHz (4G)  Separate 2400 MHz band detector for Wi-Fi/Bluetooth/Video and other latest generation devices”</p> <p>(Source: SpyCity<sup>5</sup>)</p>	<p>\$6495.00</p>

<sup>3</sup> [http://eyespyworld.com/index.php?route=product/product&path=82&product\\_id=87](http://eyespyworld.com/index.php?route=product/product&path=82&product_id=87)

<sup>4</sup> <https://hiddencamera.com.au/rfds-5-25ghz-transmitter-finder>

<sup>5</sup> <http://spycity.com.au/security/counter-surveillance/cam-105w-mobile-phone-detector/>

## **Part 1 (ii) Conclusion of market analysis**

**Research Question:** *What is the range of physical debugging equipment available on the market today?*

There is a wide variety of devices available from specialist vendors across Australia. As demonstrated above there are approximately five price-bands with devices as cheap as \$100 claiming to have bug detection features all the way through to devices that cost upwards of \$6000 and beyond. The advertising for the devices tends to emphasise the range of radio frequency (RF) signals that they detect. Most devices under \$1000 claim to detect at least up to 6 GHz, and devices over \$1000 claim they detect RF signals beyond 6 GHz. However, from the marketing claims it is difficult to decipher the performance of the devices. For instance, at what distance do they detect the various RF signals? What is the nature of the feedback provided when a positive test is detected? And how easy is it to use the device? These type of questions require further technical analysis.

## PART 2: TECHNICAL ANALYSIS

### PART 2 (i): A note on bugging devices and RF detectors

A major assumption of this research is that bugging devices used in the context of family violence are likely to use radio frequency (RF) signals for transmission. RF signals are generated by a range of devices that could be used to place someone under surveillance. This includes hidden mobile phones, Wi-Fi devices, hidden cameras, commercially available 'bugs' and other devices that communicate using RF signals. A large range of RF broadcasting devices can be used as a 'bug' that communicates video, audio or digital information to a remote observer. The working assumption of this research is that the 'bug' used by the perpetrator is generating RF signals and thus producing a trail that can be found. In other words, generating a signal that can be discovered with the suitable 'debugging' equipment.

It should be noted that it is possible for the perpetrator to use devices that **DO NOT** broadcast any RF signals. An example would be a hidden camera that records locally such as a digital video recorder. If the perpetrator has physical access to the target-location they may be capable of using a device that will not produce an RF signal. 'Bugs' of this nature can only be discovered through the physical searching of premises. It should be kept in mind that this research only relates to 'bugs' that are broadcasting RF signals.

'Bugs' that broadcast using RF signals can be categorised in many ways:

- First, according to their **broadcasting signals** such as Amplitude Modulation (AM), Frequency Modulation (FM), Digital Video Broadcasting (DVB), Global System for Mobile communication (GSM), 3G and 4G standards, Wi-Fi, Bluetooth and Digital Enhanced Cordless Telecommunications (DECT) protocols;
- Second, according to the type of **broadcasted information** such as Audio, Video, and Global Positioning System (GPS);
- Third, according to their **placement method** such as hidden in a room, placed on the persons' body, planted on the telephone line, or attached to the car; and
- Finally, according to their **transmission mechanism** either periodically (i.e., every pre-set time duration) or delayed (i.e., information stored and transmitted in short-time transmissions when specific amount of information is accumulated or when the device is queried for its information).

An RF detector (i.e. a 'bug detector') is a device that can scan the surrounding environment and show the levels of present RF signals. The scan process, which is mostly performed by an operator, requires sweeping, inspecting and probing all places in the suspected environment while watching or hearing indications generated by the RF detector device about any kind of detected RF signal. All radio waves will show an increased level of activity and will be shown or indicated by the RF detector. The operator needs to find the physical location of the highest RF level by moving the detector in different directions in order to locate the transmitter source. Once a signal is detected a closer study is needed to examine all the sources to find any illegal or malicious transmitters.






Examples of RF signals transmitting equipment are:

- DECT telephones or their base stations;
- Wi-Fi routers;
- Wi-Fi devices;
- Working mobile phones (GSM, 3G, 4G);
- Wireless video cameras;
- Child surveillance systems;
- Hidden video cameras;
- Hidden GSM/3G/Wi-Fi transmitters;
- VHF/UHF transmitters; and
- Microwave transmitters.



## PART 2 (ii): The sample

On the completion of the market analysis, five RF detectors (i.e. 'bug detector') devices were purchased. Devices were chosen within the restrictions of the budget and with the aim of acquiring equipment from multiple price bands as identified in the market analysis. The following five devices were chosen for technical analysis:

Category	Name of Sample Device	Picture	Advertising and Specification Claims	Price (including shipping and GST)
<b>Category A – Under \$100</b>	<i>Mini Pocket RF Listening Device and Camera Detector</i>		<p>Frequency Range: Up to 2.6GHZ  Detect RF bug and wireless camera signals up to 2.6GHZ  Detects wireless cameras and bugs up to 10m  Multi channel fuzzy scanning  Telephone Tap Detection  Hidden Camera Detection  Mobile Phone Detection</p> <p>(Source: OzSpy<sup>6</sup>)</p>	<p>\$29.95</p> <p>(Vendor: OzSpy)</p>
<b>Category B - \$100 to \$400</b>	<i>Versatile RF Bug and Wireless Camera Detector</i>		<p>This device can detect most GSM phone, 3G-4G smartphone, Wi-Fi, wireless bug, wireless analog, digital cameras and other wireless devices using 50 MHz - 6.0 GHz.</p> <p>(Source: OzSpy<sup>7</sup>)</p>	<p>\$195.95</p> <p>(Vendor: OzSpy)</p>
<b>Category B - \$100 to \$400</b>	<i>Protect 1203 Portable Spy Bugs Found Detector</i>		<p>Frequency range 30—6000 MHz</p> <p>(Source: SecurityLab<sup>8</sup>)</p>	<p>\$303.27</p> <p>(Vendor: Security Lab)</p>
<b>Category C - \$400 to \$1000</b>	<i>FC6002 MKII Tracer</i>		<p>Built in Speaker to Output Alert Tones  Vibration motor and earphone jack for silent detection of Listening Devices  Alarm click beep and bar graph to indicate signal strength  Frequency range is 1MHz to 6GHz  Compact size so you can take it anywhere</p> <p>(Source: OzSpy<sup>9</sup>)</p>	<p>\$489.95</p> <p>(Vendor: OzSpy)</p>
<b>Category D - \$1000 to \$2500</b>	<i>Pro4000D – Pocket Bug Detector</i>		<p>With a true frequency range of 1 to 4800 Mhz (4.8Ghz) and sensitivity that other bug detectors rarely come close to, the PRO4000D will detect and locate all types of radio transmitting bugging devices. These include battery operated transmitters or bugs, mains powered bugs, telephone bugs, video transmitters, mobile telephones, walkie talkies etc.</p> <p>(Source: SpyCity<sup>10</sup>)</p>	<p>\$1454.34</p> <p>(Vendor: OzSpy)</p>

<sup>6</sup> <https://www.ozspy.com.au/mini-pocket-rf-bug-and-camera-detector>

<sup>7</sup> <https://www.ozspy.com.au/versatile-rf-bug-and-wireless-camera-detector>

<sup>8</sup> [http://www.securitylab.com.au/professional-spy-phone-bugs-found-detector-protect-1203.html?filter\\_name=Protect%201203](http://www.securitylab.com.au/professional-spy-phone-bugs-found-detector-protect-1203.html?filter_name=Protect%201203)

<sup>9</sup> <https://www.ozspy.com.au/rf-tracer-and-bug-detector>

<sup>10</sup> <http://spycity.com.au/security/counter-surveillance/pro4000d-pocket-bug-detector/>

## PART 2 (iii) Testing the devices

Technical research analysis was conducted by Dr Samer Hanoun, Senior Research Fellow with the Institute of Intelligent Systems Research (IISRI). Dr Hanoun created a laboratory environment in which the five ‘bug detectors’ were tested for their ability to discover RF signals. A number of devices that generate RF signals were chosen to create the test conditions. These devices were also chosen for their relatively high potential likelihood of being used by perpetrators of family violence. The test experiment environment was setup using the following devices:

- A Wi-Fi router having 2 wireless networks transmitting on 2.4 GHz and 5 GHz;
- An Optus 3G mobile phone transmitting in the range 0.85 GHz to 2.1 GHz (assumed working on GSM1800 or 1.8 GHz) with its Wi-Fi and Bluetooth disabled (i.e., Off) and no call is made;
- A Vodafone 4G LTE mobile phone transmitting in the range 0.7 GHz to 2.6 GHz (assumed working on GSM1800 or 1.8 GHz) with its Wi-Fi and Bluetooth enabled (i.e., On) and no call is made;
- A laptop with Bluetooth connected to devices transmitting on 2.4 GHz; and
- An RF Explorer Signal Generator, shown in Figure 1, simulating a bug transmitting on 1.0 GHz;



Figure 1: The RF Explorer Signal Generator. Capable of producing replica RF signals that can simulate embedded ‘bug’ devices

In general, the below table shows the range of detection distances for common legal devices. These distances act as a guideline for evaluating the accuracy and sensitivity of the examined ‘bug detectors’.

Device	Detecting Distance
VHF/UHF transmitter	0.5-1m
AC powered audio transmitter	0.5-1m
Wireless camera	0.5-1m
GSM transmitter/ GSM transmitter	0.3-1m
Bluetooth	0.1-0.3m
Wi-Fi router	0.5-1m
Wi-Fi transmitter	0.3-1m
3G transmitter/ telephone	0.2-0.6m
4G (LTE) telephone	0.2-0.6m


The five ‘bug detectors’ were tested against a number of criteria. The test criteria covered both the device’s detection performance and the user-experience for operating and comprehending the device’s feedback. The test criteria were:


- Range (i.e., detection frequency range);
- Accuracy or sensitivity (i.e., detection distance and impact of background signals);
- Feedback (i.e., detection feedback either visual, audio and/or vibrations);


- Calibration (i.e., whether the device requires calibration);
- Speed (i.e., observed detection speed);
- User’s background (i.e., novice user and expert user);
- Ease of use;
- Size and Portability; and
- Clarity of manual and instructions of use


**PART 2 (iv) The results**


The following tables present a comprehensive breakdown of the test experiment results. Observations and comments for each of the ‘bug detector’ devices are also included.

<p><b>Mini Pocket RF Listening Device and Camera Detector</b></p>	
<p><b>General Specifications</b></p>	<ul style="list-style-type: none"> <li>• Detect RF bug and wireless camera signals up to 2.6GHZ</li> <li>• Detects wireless cameras and bugs up to 10m</li> <li>• Multi-channel fuzzy scanning</li> <li>• Telephone Tap Detection, Hidden Camera Detection, Mobile Phone Detection</li> </ul>
<p><b>Criteria</b></p>	<p><b>Results/Observations/Comments</b></p>
<p>Range</p>	<ul style="list-style-type: none"> <li>• RF Explorer Signal Generator detected</li> <li>• Wi-Fi router detected</li> <li>• 3G mobile not detected</li> <li>• 4G mobile not detected</li> <li>• Bluetooth detected</li> </ul>
<p>Accuracy/Sensitivity</p>	<ul style="list-style-type: none"> <li>• Does not pick any background RF signals</li> <li>• Detection distances <ul style="list-style-type: none"> <li>○ RF Explorer Signal Generator (at 5cm)</li> <li>○ Wi-Fi router (at 15cm)</li> <li>○ Laptop (at 20cm)</li> </ul> </li> <li>• Very short detection distances</li> </ul>
<p>Feedback</p>	<ul style="list-style-type: none"> <li>• Audio via beeping sound getting more solid as the transmitting source is approached</li> <li>• Visual via flashing LED</li> </ul>
<p>Calibration</p>	<ul style="list-style-type: none"> <li>• Device does not require any calibration</li> </ul>
<p>Speed</p>	<ul style="list-style-type: none"> <li>• Quick detection</li> </ul>
<p>User’s background</p>	<ul style="list-style-type: none"> <li>• Novice user can easily operate it</li> </ul>
<p>Ease of use</p>	<ul style="list-style-type: none"> <li>• Easy to use by extending its antenna, pressing down its “A” button and sweeping the surrounding area</li> <li>• The “A” button is too small to press</li> <li>• Thumb feeling uncomfortable after pressing the “A” button for a while</li> </ul>
<p>Size/Portability</p>	<ul style="list-style-type: none"> <li>• Adequate size for carrying around specially in pants pocket</li> </ul>
<p>Clarity of manual and instructions of use</p>	<ul style="list-style-type: none"> <li>• Manual not well written from a language perspective</li> <li>• Instructions of use can be better presented in the manual</li> </ul>
<p>Price</p>	<ul style="list-style-type: none"> <li>• Price (\$29.95) is very good and affordable for everyone given its basic use</li> </ul>

<p><b>Versatile RF Bug and Wireless Camera Detector</b></p>	
<p><b>General Specifications</b></p>	<ul style="list-style-type: none"> <li>• Detect wireless CCTV cameras, wireless phones, wireless bugs, Wi-Fi and 2G, 3G, 4G Cellphones from 50MHz to 6.0GHz</li> <li>• Multiple strength / level indication: Sound LED and Vibration</li> <li>• Sensitivity tuner for distance adjustment</li> <li>• Silent detection with earphones for use without others noticing</li> </ul>
<p><b>Criteria</b></p>	<p><b>Results/Observations/Comments</b></p>
<p>Range</p>	<ul style="list-style-type: none"> <li>• RF Explorer Signal Generator detected</li> <li>• Wi-Fi router detected</li> <li>• 3G mobile hardly detected</li> <li>• 4G mobile detected only on phone call</li> <li>• Bluetooth detected</li> </ul>
<p>Accuracy/Sensitivity</p>	<ul style="list-style-type: none"> <li>• Does not pick any background RF signals</li> <li>• Detection distances <ul style="list-style-type: none"> <li>○ RF Explorer Signal Generator (at 20cm)</li> <li>○ Wi-Fi router (at 100cm and also from outside the room when pointed towards the router direction)</li> <li>○ Laptop (at 50cm)</li> </ul> </li> <li>• Very short detection distances</li> <li>• Turning the sensitivity tuner to its lowest, the only device that could be detected is the router at 30cm</li> </ul>
<p>Feedback</p>	<ul style="list-style-type: none"> <li>• Audio via beeping sound getting more frequent as the transmitting source is approached</li> <li>• Visual via flashing LED on scale from Green to Orange to Red to show the signal strength of the transmitting source as it is been approached</li> <li>• Vibration mode with no audio</li> <li>• Earphone can be sued for silent detection</li> </ul>
<p>Calibration</p>	<ul style="list-style-type: none"> <li>• Device does not require any calibration</li> </ul>
<p>Speed</p>	<ul style="list-style-type: none"> <li>• Quick detection</li> </ul>
<p>User's background</p>	<ul style="list-style-type: none"> <li>• Novice users need to understand how to use the sensitivity tuner, the difference between analogue and digital signals (AD switch), devices operating on different signals</li> </ul>
<p>Ease of use</p>	<ul style="list-style-type: none"> <li>• Easy to use by extending its antenna and sweeping the surrounding area</li> </ul>
<p>Size/Portability</p>	<ul style="list-style-type: none"> <li>• Adequate size for carrying around perhaps in a jacket pocket or a bag but not in pants pocket</li> </ul>
<p>Clarity of manual and instructions of use</p>	<ul style="list-style-type: none"> <li>• Manual well written from both language and organisation perspectives</li> <li>• Instructions of use are well presented in the manual</li> </ul>
<p>Price</p>	<ul style="list-style-type: none"> <li>• Price (\$195) is moderate given its overall features</li> </ul>

<p><b>Protect 1203 Portable Spy Bugs Found Detector</b></p>	
<p><b>General Specifications</b></p>	<ul style="list-style-type: none"> <li>• Frequency range 50MHz-6GHz</li> <li>• Detects modern communications, including the GSM, 3G, 4G (LTE), Bluetooth and Wi-Fi 2.44 and 5 GHz</li> <li>• Vibrating indicator</li> <li>• Detect both analogue and digital transmissions</li> </ul>
<p><b>Criteria</b></p>	<p><b>Results/Observations/Comments</b></p>
<p>Range</p>	<ul style="list-style-type: none"> <li>• RF Explorer Signal Generator detected</li> <li>• Wi-Fi router detected</li> <li>• 3G mobile detected</li> <li>• 4G mobile detected</li> <li>• Bluetooth detected</li> </ul>
<p>Accuracy/Sensitivity</p>	<ul style="list-style-type: none"> <li>• Does not pick any background RF signals</li> <li>• Detection distances <ul style="list-style-type: none"> <li>○ RF Explorer Signal Generator (at 15cm)</li> <li>○ Wi-Fi router (solid at 50cm, intermittent from outside the room)</li> <li>○ 3G mobile (at 5cm)</li> <li>○ 4G mobile (at 5cm)</li> <li>○ Laptop (at 50cm)</li> </ul> </li> </ul>
<p>Feedback</p>	<ul style="list-style-type: none"> <li>• No audio</li> <li>• Visual via flashing LED on scale of Orange colour to show the signal strength of the transmitting source as it is been approached</li> <li>• Vibration; however not always</li> </ul>
<p>Calibration</p>	<ul style="list-style-type: none"> <li>• Device does not require any calibration</li> </ul>
<p>Speed</p>	<ul style="list-style-type: none"> <li>• Quick detection</li> </ul>
<p>User's background</p>	<ul style="list-style-type: none"> <li>• Novice users can easily use it</li> </ul>
<p>Ease of use</p>	<ul style="list-style-type: none"> <li>• Easy to use by switching it on and sweeping the surrounding area</li> </ul>
<p>Size/Portability</p>	<ul style="list-style-type: none"> <li>• Adequate size for carrying around perhaps in a jacket pocket, shirt pocket or a bag but not in pants pocket</li> </ul>
<p>Clarity of manual and instructions of use</p>	<ul style="list-style-type: none"> <li>• Manual very well written from both language and organisation perspectives</li> <li>• Instructions of use are well presented in the manual</li> </ul>
<p>Price</p>	<ul style="list-style-type: none"> <li>• Price (\$295) is above moderate given its overall features</li> </ul>

<p><b>FC6002 MKII RF Tracer</b></p>	
<p><b>General Specifications</b></p>	<ul style="list-style-type: none"> <li>• Frequency range 1 MHz - 3 GHz</li> <li>• Pocket size</li> <li>• Built-in speaker to output alert tone</li> <li>• Vibration motor and earphone for silent detection</li> <li>• 5 section RSSI bargraph to show relative RF signal strength</li> </ul>
<p><b>Criteria</b></p>	<p><b>Results/Observations/Comments</b></p>
<p>Range</p>	<ul style="list-style-type: none"> <li>• RF Explorer Signal Generator detected</li> <li>• Wi-Fi router detected</li> <li>• 3G mobile detected</li> <li>• 4G mobile detected</li> <li>• Bluetooth detected</li> </ul>
<p>Accuracy/Sensitivity</p>	<ul style="list-style-type: none"> <li>• Increasing sensitivity causes the device to have solid detection and always vibrating which does not reflect or show whether these are background signals or a transiting source. At this stage the sensitivity button need adjustment to determine a suitable direction to pursue</li> <li>• Detection distances <ul style="list-style-type: none"> <li>○ RF Explorer Signal Generator (at 20cm on moderate sensitivity)</li> <li>○ Wi-Fi router (solid at 50cm and intermittent from outside the room on moderate sensitivity)</li> <li>○ 3G mobile (at 15cm increased with increasing the sensitivity)</li> <li>○ 4G mobile (at 15cm increased with increasing the sensitivity)</li> <li>○ Laptop (at 20cm on moderate sensitivity)</li> </ul> </li> </ul>
<p>Feedback</p>	<ul style="list-style-type: none"> <li>• No audio</li> <li>• Visual via flashing LED on scale of Red colour to show the signal strength of the transmitting source as it is been approached</li> <li>• Vibration only when neat by the transmitting source</li> </ul>
<p>Calibration</p>	<ul style="list-style-type: none"> <li>• Device does not require any calibration</li> </ul>
<p>Speed</p>	<ul style="list-style-type: none"> <li>• Quick detection</li> </ul>
<p>User's background</p>	<ul style="list-style-type: none"> <li>• Novice users can easily use it however, it is hard to understand the relationship between the sensitivity adjustment and detection</li> <li>• More suitable for expert users</li> </ul>
<p>Ease of use</p>	<ul style="list-style-type: none"> <li>• Easy to use by switching it on and sweeping the surrounding area</li> </ul>
<p>Size/Portability</p>	<ul style="list-style-type: none"> <li>• Adequate size for carrying around perhaps in a jacket pocket or a bag but not in pants pocket</li> </ul>
<p>Clarity of manual and instructions of use</p>	<ul style="list-style-type: none"> <li>• Basic manual</li> <li>• Lacks adequate instructions of use</li> </ul>
<p>Price</p>	<ul style="list-style-type: none"> <li>• Price (\$440) is way higher given its overall features</li> </ul>

<b>Pro-4000D Pocket Bug Detector</b>	
<b>General Specifications</b>	<ul style="list-style-type: none"> <li>• 4.8 GHz Wide Frequency Response</li> <li>• High Sensitivity to locate the weakest signals</li> <li>• Audible Signal Strength 'Beep'</li> <li>• Audio Demodulation</li> <li>• Flexible 'whip' Antenna</li> <li>• Low Battery Indicator</li> </ul>
<b>Criteria</b>	<b>Results/Observations/Comments</b>
Range	<ul style="list-style-type: none"> <li>• RF Explorer Signal Generator detected</li> <li>• Wi-Fi router detected</li> <li>• 3G mobile detected</li> <li>• 4G mobile detected</li> <li>• Bluetooth detected</li> </ul>
Accuracy/Sensitivity	<ul style="list-style-type: none"> <li>• Very sensitive</li> <li>• Solid detection as flashing LEDs are solid and stable while detection is in place. Scale and beeping increase when approaching the transmitting source</li> <li>• Detection distances <ul style="list-style-type: none"> <li>○ RF Explorer Signal Generator (at 20cm)</li> <li>○ Wi-Fi router (solid at 50cm and solid from outside the room and when approaching the room)</li> <li>○ 3G mobile (at 15cm)</li> <li>○ 4G mobile (at 15cm)</li> <li>○ Laptop (at 30cm)</li> </ul> </li> </ul>
Feedback	<ul style="list-style-type: none"> <li>• Audio beeps</li> <li>• Visual via flashing LED on scale of Green colour to show the signal strength of the transmitting source as it is been approached</li> <li>• No vibration</li> </ul>
Calibration	<ul style="list-style-type: none"> <li>• Device does not require any calibration</li> </ul>
Speed	<ul style="list-style-type: none"> <li>• Quick detection</li> </ul>
User’s background	<ul style="list-style-type: none"> <li>• Novice users can easily use it</li> </ul>
Ease of use	<ul style="list-style-type: none"> <li>• Easy to use by switching it on and sweeping the surrounding area</li> <li>• On/Off button for beeping audio</li> </ul>
Size/Portability	<ul style="list-style-type: none"> <li>• Adequate size for carrying around perhaps in a jacket pocket or a bag and may fit in pants pocket</li> </ul>
Clarity of manual and instructions of use	<ul style="list-style-type: none"> <li>• Well written manual</li> <li>• Adequate instructions of use</li> </ul>
Price	<ul style="list-style-type: none"> <li>• Price (\$895) is way higher given its overall features; however it is adequate given its sensitivity and accuracy of detection</li> </ul>

## **PART 2 (iv) Conclusion of technical analysis**

### **Research Question - *What are the capabilities of physical debugging equipment?***

In this research study, different bug detection devices were analysed subject to their technical specifications as advertised by either their manufacturer or wholesaler. In addition, these devices were tested on detecting different types of transmitting sources and examined against multiple criteria.

In conclusion,

- Each of the examined devices has its pros and cons whether on accuracy, ease of use or price;
- Accuracy and price are the most critical criteria. It is apparent that these should be linearly related; however, this is not the case within the sample set as some devices are higher in price but this is not reflected within their accuracy;
- Ease of use and clarity of manual and instructions are the least critical criteria. Users can adapt easily to using new devices and can look up additional information on how to use a device in the event that the manual does not provide the required information; and
- The context of the application of these devices is highly determinant on which device to purchase.

With further time and resources, it would be ideal to get additional information about the signal detected, its frequency range and quantitative signal strength against the device direction or location of transmitting source.



## PART 3: LEGAL ANALYSIS

### PART 3 (i): Surveillance, bugs and legal definitions of family violence

The analysis of the legal framework governing stalking, tracking and the use of surveillance devices in the context of family violence employs a number of key legal definitions.

The definition of 'family violence' in section 5 of the *Family Violence Protection Act 2008 (Vic)* includes behaviour by a person towards a family member where that behaviour—

- (i) is physically or sexually abusive; or
- (ii) is emotionally or psychologically abusive; or
- (iii) is economically abusive; or
- (iv) is threatening; or
- (v) is coercive; or
- (vi) *in any other way controls or dominates the family member and causes them to feel fear for their safety or wellbeing of that of another.*

Similarly, s 4AB of the *Family Law Act 1975 (Cth)* defines family violence for the purposes of the Act as 'violent, threatening or other behavior by a person that coerces or controls a member of a person's family (the family member), or causes the family member to be fearful.'

Definitions of stalking also frequently specify prohibited conduct. For instance, in Victoria prohibited stalking includes keeping the victim (or any other person) under surveillance with the intention of causing physical or mental harm to the victim, or of arousing apprehension or fear in the victim for their own safety or that of another: *Crimes Act 1958 (Vic) s 21A(2)(f)(ii)*.

Consequently, it is clear that surveillance and technology-facilitated abuse may, according to circumstances, constitute stalking, family violence or (as will subsequently be established) other criminal offences.

### PART 3 (ii): The prevalence of technology-facilitated family violence and abuse

A survey of 46 victims of intimate partner stalking and 152 domestic violence workers in 2012 suggested that 82% of victims experienced technology-facilitated stalking, during and/or after their relationship with their abusive intimate partner<sup>11</sup>. The stalking commonly involved unwanted contact through text messages to their smart/mobile phones (82%); contact through social media, including Facebook 82%); email (52%); and the use of GPS (29%). Compared to data from past studies, there was an increasing trend toward stalking via social media. Most victims (84%) indicated that the contact had impacted their mental health and wellbeing.

Another survey of 546 domestic violence workers in 2015 indicated that they believed that 98% of their clients experience technology-facilitated abuse, during and/or after their relationship with their abusive intimate partner<sup>12</sup>. The abuse was most commonly perceived as being perpetrated via text messages and Facebook posts. Other commonly reported abuse included:

- Using GPS in cars and phones to track locations and activities (about 1/3 of respondents saw this 'often' or 'all the time' in their work)
- Using covert applications and devices on their phones to monitor and record conversations and text messages
- Hacking of email and social media

<sup>11</sup> D Woodlock, *Technology Facilitated Stalking: Findings and Recommendations From the SmartSafe Project*. Domestic Violence Resource Centre, Victoria, Collingwood.

<sup>12</sup> ReCharge: Women's Technology Safety, Legal Resources, Research & Training, 2015.

- Monitoring their internet use
- Disabling their internet connection

Numerous law cases report the use of technology to facilitate stalking and other forms of abuse, including both criminal and family law matters.

<b>Criminal law case involving technology-facilitated stalking</b>	<i>Gale v The Queen</i> [2014] VSCA 168	Accused used GPS and listening devices to track his estranged wife and her partner. Convicted of stalking and other offences.
--	---	---

<b>Family Law cases involving technology-facilitated stalking</b>	<i>Ahmed v Jeret</i> [2016]	FamCA 442: ex-partner stalked wife through false Facebook identity.
	<i>Delucca &amp; Decarlo</i> [2016]	FamCA 497: ex-husband placed tracking device on ex-wife's car
	<i>Casano v Antipov</i> (No 3) [2016]	FAMCA 1884, 10 August 2016 Hannam J. Ffather downloaded app on phone to track mother's location and monitor her calls, then monitored her Skype and email accounts, facebook, and phone. Following separation, the father hired a private investigator to keep surveillance on mother. This included surveillance of the rear entry of her home, her partner, her private activities and at her child's child care centre.
	<i>Morein v Morein</i> [2014]	FAMCA 1004, 30 October 2014 Loughnan J: Applicant obtained order restraining her ex-husband from using software to spy on her or use other forms of surveillance on her computer and other IT devices and in her motor vehicle.
	<i>Newitt v Falcone</i> (2012)	49 Fam LR 596, Cronin J: Recording device placed in ex-wife's bag after separation to overhear conversation with solicitor.

### PART 3 (iii): The legal regulation of technology-facilitated family violence and abuse in Victoria

The multiple ways in which technology-facilitated family violence can be perpetrated is matched by an equally diverse array of laws that make such activities unlawful. The following reflects a summary of the relevant legislation within Victoria for regulating technology-facilitated family violence:

<p style="text-align: center;"><b>STALKING</b></p> <p>Stalking laws prohibit a diverse range of behaviours that cause psychological harm to a victim or cause them to fear for their safety or that of another person.</p>	<i>Crimes Act 1958 (Vic) s 21A</i>	Prohibits the stalking of another person; stalking includes a range of behaviours (following, putting under surveillance etc) and can be perpetrated directly as well as by text, email etc.
	<i>Personal Safety Intervention Orders Act 2010 (Vic)</i>	

		Permits a person to obtain a <i>Personal Safety Intervention Order</i> that prohibits another person from stalking them.
--	--	--

FAMILY VIOLENCE INTERVENTION ORDER	<i>Family Violence Protection Act 2008 (Vic) ss 42-49.</i>	Threatening or coercive behaviour and behaviour that is controlling or dominating and causes a person to fear for their safety or well-being when performed by a partner or ex-partner may provide the basis for the victim to obtain a <i>Family Violence Intervention Order</i> . These orders can include conditions such as prohibiting an ex-partner from following the victim or keeping her under surveillance, etc.
------------------------------------	--	---

SURVEILLANCE Surveillance laws prohibit the use (in specified circumstances) of devices for data surveillance, listening, tracking and optical surveillance	<i>Surveillance Devices Act 1999 (Vic) ss 3, 6-8.</i>	Surveillance laws such as the <i>Surveillance Devices Act 1999 (Vic)</i> prohibit the use of listening devices, optical surveillance devices, and tracking devices in specified circumstances.
--	---	--

COMMUNICATION LAWS Commonwealth Communication Laws make it unlawful to make threats to kill / seriously harm, or to menace / harass / cause offence by telephone, internet etc	<i>Criminal Code Act 1995 (Cth) ss 474.17, 477.3(1), 478.1(1).</i>	Makes it an offence to use telecommunication services (such as that involving mobile telephones) to make threats or to Intercept or to interfere with another's communications
	<i>Telecommunications (Interception and Access) Act 1979 (Cth)</i>	

'REVENGE PORN' LAWS	<i>Summary Offences Act 1966 (Vic) s 41A-DB</i>	'Revenge porn' laws makes it an offence to capture, distribute/ or threaten to distribute an intimate image in circumstances where it would not be reasonable to do so
---------------------	---	--

RECKLESS ENDANGERMENT	<i>Crimes Act 1958 (Vic) ss 22, 23.</i>	Makes it an offence to engage in reckless conduct that places another person in danger of death or serious injury.
-----------------------	---	--

### **PART 3 (iv): Evidence gathering for criminal prosecutions**

It is important that evidence of technology facilitated family violence be obtained and retained so that it can be used in any subsequent criminal prosecutions or civil actions. Defence lawyers sometimes claim that victims generate cases based 'on lies and exaggeration'<sup>13</sup> so it is important that victims document and have records of the abuse that they have experienced.

Preservation of evidence for the purpose of criminal or civil proceedings requires that:

- Victims record the time and date on which the technologically facilitated abuse occurred
- Photographic records be created of unlawful tracking devices and other hardware in situ
- Original abusive or threatening messages be retained where possible
- Screenshots of offending messages, posts or images be obtained and retained
- Names and addresses of witnesses to relevant offending should be obtained

### **PART 3 (v): Conclusion**

**Research Question - *What are the legal implications when a 'bug' is discovered?***

Stalking and other acts of surveillance in the context of family violence is unlawful. There are numerous laws that prohibit such behaviour, depending on the offender's conduct and the circumstances of the offending. In the event that stalking, unlawful surveillance or some other related offence has occurred, it is recommended that the laws previously identified be taken into account when considering possible action that can be taken against an offender. Appropriate legal action will be context-specific to individual cases. Victims and case workers should be made aware of the importance of obtaining and retaining evidence. In the first instance, photographs of the tracking device or hardware should be created where possible. Records should be kept about the discovery of the bug and any other relevant details noted.

---

<sup>13</sup> Ly Lawyers, *Use Carriage Service to Menace, Harass or Offend*: <https://lylawyers.com.au/criminal-law/criminal-offence/use-carriage-service-to-menace/>