National Motor Vehicle Theft Reduction Council

Review of Aftermarket Devices

Autowatch Ghost CAN Immobiliser

October 2019

PREPARED BY:

IAG Research Centre

Informing Australia on vehicle crime.

Report outline

Date	October 2019
ISBN	978-1-876704-56-8
Title	Review of Aftermarket Devices
Address	National Motor Vehicle Theft Reduction Council Suite 1, 50-52 Howard Street North Melbourne Victoria 3051
Email	info@carsafe.com.au
Type of report	Product review
Objectives	To test the safety, security and effectiveness of third party immobilisers

Summary

The NMVTRC has partnered with the IAG Research Centre to conduct research and obtain expert advice on technological advances in vehicle theft methods and cyber security risks, including practical testing of select, aftermarket security devices and/or Original Equipment Manufacture security features. In this instance, IAG Research was engaged to review the Autowatch Ghost immobiliser.

The 'Ghost' is an aftermarket CAN bus immobiliser which enables motorists to encode a unique, changeable, PIN using select vehicle controls such as those on the steering wheel, door panels or centre console. The PIN must be entered in order to start the car.

The operation of this device works such that if the keys to a car were stolen and entry to the vehicle gained, the thief would still not be able to start the vehicle unless the correct PIN code was entered.

Research and tests were conducted by members of the IAG Research Centre.

The test results reflect a snapshot in time and are accurate for the vehicle make, model and device version stated. Results may vary if any of these factors are changed, or if tested under a different set of conditions.

Contents

1. Introduction 1

2. Background 1

3. Scope 2

4. Product Claims 3

5. Security and Tamper Resistance 4

6. User Friendliness 4

7. Ease of Installation 5

8. How it Works 5

9. Dependencies 5

10. Associated Costs 5

11. Other Considerations 6

12. Conflicts with Product Claims 8

13. Recommendations 10

14. Conclusion 10

1. Introduction

The following document is designed to provide insight and analysis on the Autowatch Ghost immobiliser, a device that is aimed at providing an additional layer of security and which prevents vehicle theft even if the thief has access to the car keys. It should be noted that this product is also sold in Russia and parts of Europe under the brand "Author IGLA 200 (and variants)" and comes packaged with the English version of their operating manual.

The Ghost immobiliser we received was a first-generation model that doesn't have the same functionality as the next generation model, the Ghost-II. The findings in this report are based on the first-generation model alone.

The device we received came pre-configured and set up for one of our vehicles, a 2017 Mazda CX-3.

2. Background

To provide context to this report, it is important to understand what an immobiliser is and how it works. An immobiliser is a modern anti-theft method whereby inserting the key into the ignition switch triggers a process of authorisation and verification between vehicle and key.

Engine immobilisers prevent the engine from starting and running by immobilising one or all of three main engine circuits: - the starter motor, the ignition, or the fuel pump. The engine will only start if the electronic codes sent between the vehicle and the key match.

The Ghost immobiliser is designed for situations where the thief has obtained the car keys (thus rendering the built-in immobiliser redundant) by adding another layer of security.

Since the introduction of the immobiliser as standard equipment for all new cars in Australia in July 2001, the overall rate of vehicle theft has been in decline. However, changes in theft methods which has seen thieves entering homes in order to steal car keys has resulted in a renewed interest in after market security devices. In 2018, 79 per cent of vehicles stolen in Australia were equipped with an Australian-standards equivalent immobiliser.

3. Scope

The IAGRC was engaged by the NMVTRC to assess the Ghost immobiliser on its utility, security and tamper resistance, user friendliness, ease of installation and value for money . The primary objective of the research was to test the accuracy of manufacturer claims regarding the capabilities of the Ghost immobiliser. The manufacturer claims are detailed in the following section of the report.

The following points outline the criteria on which the product was assessed:

1. Utility
Does it do what the manufacturer claims? Y/N

2. Security & Tamper resistance
Is it difficult to bypass, defeat or mask? Score: 1-5 (not very secure-very secure)

3. User friendliness
Is it simple to operate? Score: 1-5 (very Simple-very complex)

4. Ease of installation (for a professional auto electrician or vehicle security specialist)
How easy is it to install and approximate time? Score 1-5 (very simple-very complex). Time: Actual estimated

5. Dependencies
What non-device dependencies does it rely on, i.e. third part infrastructure or practices

6. Value for money?
Cost relative to 1-5 above.

7. Other considerations
Are there any other potential impacts to consider, such as OEM car warranty?

In Scope

Analysis of ability to hide from diagnostics kits

Testing bypass resistance

Radio signals emissions discovery

PIN code stress tests

Range and useability of the mobile app

Explore warranty considerations

Installation methods and best practices

Testing of additional features, e.g. Valet mode

Out of Scope

Testing any version of the device other than the one we received

Testing any vehicle other than the one mentioned in this document

Analysis of machine-code running on the device

Analysis of data security and related networks and servers

Corrosion, impact, humidity and atmospheric pressure tests

Electromagnetic capability testing

4. Product Claims

Please note that the following abstract has been taken from the Dynamco website:

"The Ghost is the world's first aftermarket CAN bus immobiliser. Protect your car from theft like nothing else on the market today.

The Ghost protects your car from key-cloning, hacking, and even key theft. The only way a thief could take a Ghost protected car is by physically towing it away, even then they will never be able to drive it! The Ghost has no key-fobs or LED indications to give away its location. The Ghost uses the buttons in your vehicle such as those on the steering wheel, door panels or centre console, to allow you to make a unique, changeable, PIN code sequence that must first be entered before you can drive your car. Just like your credit card but you can make your car PIN even safer by making it up to 20 presses long!

However, we did not settle there! In order to make extreme security also be hassle free, we have created an iPhone application that connects to your car and allows you to get in and drive without having to enter the PIN code. This iPhone pairing allows a single, authorised, connection with a secret pairing code that is unique to every Ghost and communication between the Ghost and the iPhone is encrypted. All you have to do is pair your iPhone with your Ghost, leave the Autowatch Ghost application running in the background with Bluetooth enabled and you can drive conveniently and securely.

Features

- *Immobilisation by communicating with the ECU*
- *PIN code via buttons on steering wheel / dash*
- *Undetectable using diagnostics*
- *Cannot be bypassed using standard theft methods*
- *No radio frequency signals*
- *No additional fobs (commercial vehicle option allows for fobs)*
- *Uses the on-board CAN data network*
- *Unique user changeable PIN code*
- *Service / Valet mode means the PIN code is never compromised*
- *Secure, unique emergency code should the PIN be forgotten"*

5. Security and Tamper Resistance

Pros	Cons
The housing for the unit is of high quality. It is cased in two layers of material, making it air tight and waterproof, to help protect it and to keep it looking as inconspicuous as possible.	The wiring harness is colour-coded, presumably to make it easier to install. This has the effect of making it easier to discover. Other devices of similar function use black wires only.
The Ghost immobiliser does not use wireless technology in the common 433MHz range, meaning it does not transmit or receive any signals and is impervious to traditional attacks we would use on RF devices such as jamming, relaying or replay attacks.	Cutting or disconnecting any one of the four wires connected to the OBD will disable the Ghost immobiliser without affecting the operation of the vehicle.
It does not emit sounds or lights, as with other similar devices, and thus hard to find quickly. There is no dash illumination until the correct sequence has been entered.	It has the option for Bluetooth compatibility which adds an attack vector in the 2.4GHz range. This would potentially allow an attacker to gain access to the vehicle via that open channel. This cannot be tested further at our facility until we have proper signal shields in place, i.e. purpose-built Faraday cage for signals testing.
Even in the case that a thief knew about the installation and the PIN was only 4 presses in length, the number of combinations they would have to guess would likely be too many to effectively brute force.	There is no consideration for repeated incorrect attempts, an attacker would potentially have an unlimited number of incorrect attempts for guessing the PIN.
There is no evidence to suggest that the immobiliser is prone to packet injection via the CAN bus.	
The device could not be detected using diagnostic tools.	

Bypassing	1	2	3	4	**5**
Defeating	1	**2**	3	4	5
Masking	1	2	3	4	**5**
Overall Score	**1**	**2**	**3**	**4**	**5**

Meaning: This device's greatest strength lies in its stealth and obscurity but is relatively easy to defeat once located. If it remained undiscovered it could be near impossible to break. The reason it does not receive a rating of '5' is because if it was found, disabling it completely only requires any one of the wires being cut.

6. User Friendliness

The procedure to operate the device is quite simple and feels natural in doing so. The driver simply turns on the ignition (without starting the engine), enters their unique code and, if successful, the indicators will flash twice, allowing them to start the vehicle. The only aspect that seems cumbersome is if the user has a long PIN to remember and enters it each time they require use of their vehicle. It should be noted that additional security generally comes with less convenience.

Regarding the mobile application, it performed as stated. There is support for an iPhone to be connected via Bluetooth, and this was easy to get set up and running, however there is no support for Android devices on the first-generation models (this was added for the Ghost-II).

Being able to leave the app running in the background is a nice feature as it allows you to start the vehicle without having to enter your PIN, if the phone is within close proximity to the vehicle. This feature is not required to be used and the app can be turned off with full functionality of the device remaining.

The app itself had an effective range of 16 metres.

Changing a PIN code or entering Service mode is also a straightforward procedure, and it is our opinion that this can be easily achieved by the average user.

7. Ease of Installation

Setting up the device

Before installation, the Ghost needs to be set up for each specific vehicle. Part of this process requires a login to the portal for authorised installers, where they then download the required software. This step would be included as part of the installation and not something a customer would have to be concerned with.

Please note that this product is only offered as supply and fit through a network of authorised dealers. It is not available as a separate unit and cannot be purchased and fitted by an enthusiast.

Time to install: 30 mins for a basic setup, longer for a more incognito design, for example, tucked away under the dash or engine bay. Generally, the better hidden, the longer the installation time.

Process:

1. Removal of trims (5 mins)
2. Solder wires as in diagram supplied with device (12 mins)
3. Learn the new PIN code (4 mins)
4. Confirm serial number (4 mins)
5. Immobilisation confirmation tests (5 mins)

Following the instruction manual, an authorised installer should have no issue installing, provided they:

(a) Know the location of the CAN bus
(b) Know the pin layout of the CAN bus
(c) Follow the instruction manual accordingly

For ease of demonstration, we decided to wire the device directly into the CAN bus under the driver's dash, but in theory the device could be better hidden elsewhere in the vehicle.

How easy is it to install? (Time to install: 15 mins)	**1**	**2**	**3**	**4**	**5**

Meaning: It is very easy to install, the instructions are straightforward, and does not take long to complete the job. Removal of the device is also a simple task.

8. How it Works

In simple terms, how it works is when the Ghost receives a signal that tells it the car wants to start but the correct code has not been entered, it sends out a pre-defined signal to the CAN bus to shut the engine down (or in some cases, locks the transmission instead).

Although we cannot determine the exact signal being used in this instance, usually the signal used will be of high importance, such as the signal that would be used to detect a "serious collision", which will trigger a response from the vehicle to enter its protection mode, without causing a fault code or engine warning lamp.

9. Dependencies

Since this device uses the CAN bus to immobilise the vehicle, the vast majority of fittings will be located upstream of the OBD-II diagnostic connector (SAE J1962 Type A) but can be fitted in the engine or boot compartment.

Before installation, the Ghost needs to be set up for the specific vehicle. Part of this process requires a login to the portal for authorised installers, where they then download the required software. (If the device has come fully set up and only requires installation then this step is not necessary.)

10. Associated Costs

In Australia, to purchase and install the product can range from $700-$1000.

There is also the option to transfer ownership from vehicle to vehicle (if you sell your car and want to put the Ghost immobiliser on your next vehicle). The quoted cost of doing so (through another installer) is approximately $550.

All products sold by Dynamco (the Australian distributors) come with a 2-year Limited Warranty for devices purchased in Australia. It is advised to read the full Terms and Conditions for more information.

11. Other Considerations

Manufacturer Warranties

During our investigations, we came across claims that guaranteed the product would not void the manufacturer warranty. We therefore sought the car manufacturer's viewpoint on the installation of aftermarket devices regarding warranties. We posed the following questions:

1. Does installation of aftermarket immobilisers void the manufacturer warranty?
2. Does it make a difference if it has been installed by an authorised installer?
3. If something with the electrics broke, would the aftermarket device likely be blamed for the fault?

The manufacturer responses were unanimous that:

- Yes, the warranty will be voided;
- No, it does not make any difference if they were an authorised installer; and
- Yes, any aftermarket installation would likely be looked at as the source of a fault.

"Just the introduction on a non-manufacturer electrical / electronic component into the vehicle's electrical system can cause disturbance to the BUS / CAN systems, let alone physical damage to various electronic control units".

There was also comment made regarding non-electrical components, "(as the manufacturer) *we couldn't not pay for a faulty door trim if it has a non-genuine immobiliser fitted but if they removed the door trim to install – we wouldn't cover it."*

Any addition to the electrical system of a vehicle has potential to cause issues. In fairness, this may not be a major concern for those vehicles that are already out of warranty or several years old, but caution should still be taken from a safety (and financial) perspective as it could adversely affect other systems within the vehicle.

Our advice to the consumer is if voiding the manufacturer warranty is of concern to you, we suggest contacting your manufacturer or local dealer and get their advice before installing any aftermarket equipment.

Forgetting a PIN

There is also a consideration regarding forgetting the PIN.

The process for recovery of the vehicle in such an event is possible and requires the emergency card that is provided in the box. The instructions for recovering the vehicle are on the reverse side of the card and allow you to input a new PIN.

This would seemingly not be ideal in some emergency-like situations where escaping some form of risk or danger requires immediate use of the vehicle, or if the driver (who is the only one that knows the PIN) is incapacitated.

A solution to this problem that one installer is providing is to give the customer the option of installing a kill switch in a hidden location, which overrides the immobiliser in the event of an emergency. However, this has the caveat of having something within the car that defeats the purpose of the having an immobiliser.

Smartphone Compatibility

We tested the claims that the device is compatible with iOS and found the setup was simple and worked straight away. The process for enabling the service via the app is very straightforward and we can see how some people would make beneficial use of this function. However, purely from a security standpoint, it would add an attack vector into the vehicle through Bluetooth, and is not recommended.

The app had an effective range of 16 metres, meaning that if the keys were inside or in close proximity to the car, the phone running the app could be 16 metres away and the car could still be started and driven away. This has possible security implications when at a café, restaurant, service station or any other scenario where you are within a close distance to your parked vehicle and may have left the app running in the background with the vehicle unlocked.

We also tested the app itself, by trying to pair a second iPhone to the vehicle but found only one phone was being accepted at a time. To pair with the vehicle also requires a Bluetooth pairing code that is found on the emergency card which increases the security. Adding and deleting paired devices is only done so via the app.

This feature has an obvious caveat regarding multiple users, for example, a shared vehicle between partners. Only one person will have use of the feature at a time, and so in order for them to switch between who gets smartphone access, they would have to do the entire process of deleting the existing connected device and adding a new one. There is evidence to suggest this has been fixed to allow for two phones to be paired in the Ghost-II but we are unable to confirm this.

Support for Android devices is only available on the Ghost-II. Our tests are being performed on a first-generation device which explains the discrepancy in not testing Android.

Australian Standards

Vehicle Standard (Australian Design Rule 82/00 - Engine Immobilisers) 2006 makes no mention of items the device is in breach of, so it is safe to say it is compliant with these measures.

However, it does appear to fail AS NZS 4601:1999 in the following sections:

2.2.12 Wiring

All primary wires emanating from and connecting to the VSIS control unit shall be black in colour and of the same diameter. There shall be a minimum of nine black coloured wires emanating from/connecting to the control unit. All installation labels shall be removed after installation. Plugs and sockets concerned with the primary wires shall be fully contained by the VSIS control unit housing.

2.2.8 Immobilisation

The VSIS shall meet the following requirements:

(a) Immobilisation shall be via at least two independent systems, whether contained within the control unit or within external sealed systems code-linked to the control unit, acting on either the starter or fuel or ignition, or engine management system preventing movement of the vehicle under its own power.

In the test sample it appears that the immobiliser disabled the engagement of the starter motor only.

The standard is twenty years old now and advances in technology may render some of it in need of updating, however, it should be noted that the immobiliser fails AS NZS 4601:1999 in its current form.

The other point to note is that this device is not intended to be a standalone immobiliser. It sits as an added layer of security in the vehicle – that is, there is still an immobiliser fitted from the OEM that is compliant with both measures.

Bluetooth

Bluetooth aspects could not be thoroughly tested due to limitations in our testing environment. Since Bluetooth exists in the 2.4GHz range, it is imperative that tests be conducted in a Faraday cage to protect the public and avoid legal ramifications. We did manage to capture the signal being emitted but could not transmit on this frequency, as a result, test outcomes do not take Bluetooth attacks into consideration.

Other Cyber Safety Aspects

It should also be noted that there may be unknown effects on other systems resulting from connecting another device to the vehicle's CAN bus system. Some of these include effects from the extra current draw and possible fault code injection, but testing these effects is outside the scope of our work.

The number of known risks that cannot be tested due to current limitations in our skill level, equipment, processes, scope of work, and allowable timeframes, are numerous and can include a range of items such as back to base communications, data retrieval, snooping, and unwanted vehicle tracking.

Lastly, there is a possibility of several unknown risks that can potentially have ramifications. The cyber domain is vast and it is virtually impossible to track *every* vulnerability and weakness; therefore the focus becomes more about likelihood and estimated effectiveness in reference to time. Generally, a system only needs to be robust enough that the time/effort taken to break it outweighs the reward of doing so.

Testing Limitations

These tests have been performed on a single vehicle (Mazda CX-3), thus all findings are limited in being connected to this car alone. We cannot say definitively that the results would be identical for different makes and models. In different or more

sophisticated vehicular networks, there may be additional unwanted behaviours that are unknown due to this testing limitation.

12. Conflicts with Product Claims

Length of PIN

We tested the claims that the PIN can be any length of between 3 and 20. Whilst the lower limit was found to be correct at 3, we found that we could go beyond the upper limit to 22. At this time, we cannot determine if this is intentional, oversight, a software bug or a glitch.

Service Mode

There is also an issue of there being an inconsistent timeout time for disabling Service mode. The handbook states that

"Service mode can be deactivated manually by entering the PIN, or automatically when you finish driving and the speed during your ride had reached 50 km/h at least once and the car had been in motion at least 3 minutes without stops (or stops that were not longer than 3 minutes).

The double indication signal will show that the service mode is deactivated."

Our tests showed an inconsistency in these times, with recorded times of 19:45, 17:58, 17:04, 15:28 and 23:40. We also tested in different driving environments but found no correlation to an increase or decrease in times before deactivation. We cannot be certain at this time of the cause or potential implications of this discrepancy.

Through our open-source investigations, we came across claims that this has been recently updated to allow for up to 15 minutes of drive time, which is a closer reflection to our own test results, although we were still able to go beyond that time on each occasion.

Country of Origin

At the time of writing, the Autowatch website claims that "*Autowatch is the distributor of PFK Electronic equipment, designed and manufactured from its own factory*".

During our open-source reconnaissance of this device, we tracked the original product to belonging to a Russian company called автор (translated: Author) and branded as a model called the "IGLA". On the company website, they claim that their products are assembled in St. Petersburg.

PFK Electronics, which is based in South Africa, supply the device to the UK via their distributors Autowatch UK. A company called Dynamco (based in Perth, Australia) has supplied it to the NMVTRC and is listed as a distributor on PFK Electronics' website.

Everything comes branded "Author IGLA" out of the box, including instructions and the device itself. Upon opening the casing, we discovered the circuit board was stamped as Author IGLA, assembled in 05/2016.

Range of Options

The full range of options is dependent on the vehicle that the device has been installed in. The following table highlights what features are available on the Mazda CX-3 that we used for testing.

Test Results for Options

Option	On	Off	Comment
Service mode	5	Automatically or by entering your PIN	Works as expected, but the timeout is inconsistent
Opening of a central lock	6	7	Not featured
Closing of a central lock above 10km/h	8	9	Not featured
Ventilation	10	11	Not featured
Comfort	12	13	Not featured
Mirror fold	14	15	Not featured
Anti Hi-jack	16	17	Not featured
Engine start disabling	18	19	Not featured
Additional option	20	21	Not featured
Transport mode	See manual for process		Works as expected, a handy feature to have

Note: greyed boxes indicate the default setting, unless specified otherwise

It is unclear at this time if the consumer is made aware of what additional features they will receive. However, a full feature list is available to the distributors via an online portal, and this information could potentially be passed on to customers if queried.

At the time of writing, there is no option to purchase additional features, for example, the extra modules that are currently available to some European customers. Once again, further information about the extra modules is outside the scope of this report.

Simplicity of operation?	1	2	3	4	5

Meaning: Operations such as changing a PIN or putting the device into service mode are very straightforward and the manual provides a step-by-step guide that is easy to follow. Even though inputting a 20-length PIN becomes tedious, the process is still very simple.

13. Recommendations

- Reduce the maximum number of presses for the PIN to 8. It is not considered practical to have a PIN greater than this and it does not substantially affect the likelihood of theft. Recommended size for practicality is between 4 and 6.
- Change the coloured wires to black or cover them in black electrical tape during installation. This will add to its ability to blend in with its surroundings and in meeting AS NZS 4601:1999 section 2.2.12.
- Include a transparent list of features for each make and model. Currently this can only be done through the authorised distributor portal.
- The ability to choose where the Ghost gets positioned within the vehicle. The device comes with a guideline as part of the installation instructions, but if you would like it hidden in a different location, it might be worth negotiating this with the installer. The implication here is that once you know the location in one vehicle, other vehicles of the same model will likely have the Ghost positioned in the same place, and the device will lose its greatest strength - invisibility.

14. Conclusion

The Autowatch Ghost immobiliser is a simple and effective device that helps to enhance the theft-resistance of a vehicle, and is small, discrete and easy to operate.

In most cases, the device would assist in preventing opportunistic vehicle theft where the thief has gained access to the car keys. The inability to start the car would likely make would-be thieves believe there was something wrong with the car, and result in them moving on to another target. However, for a sophisticated attacker who knew what to look for and possessed the tools and knowledge of how to disable the device, it would simply represent another hurdle to overcome.

Overall, we conclude that installation of the Ghost immobiliser provides an effective, added layer of security to a vehicle and has the potential to reduce the majority of vehicle theft where the car is stolen using the keys.

Does it meet the manufacturers claim?	Yes	No

Meaning: Our testing proved enough criteria, beyond a reasonable standard, to satisfy the manufacturers claims.