# Inquiry into Reports of
# Unlawful Surveillance of
# Garda Síochána Ombudsman Commission

## REPORT

## By


## Judge John D. Cooke

**(High Court – Retired)**


**To: An Taoiseach**
**Government Buildings**
**Dublin 2**

**4th June 2014**

Contents

# 1. Introduction

1.1. This is the report of the Independent Inquiry into Reports of Unlawful Surveillance of the Garda Síochána Ombudsman Commission as appointed by the Government on 19th February 2014 and approved by resolution of Dáil Eireann of that date. By letter of 26th February 2014 I was informed of my appointment to conduct that Inquiry by the Secretary General to the Department of the Taoiseach.

1.2. The appointment was accepted by me by letter of 28th February 2014 to the Secretary General and my indication of the terms upon which I understood the Inquiry was to be carried out given in that letter was accepted by the Secretary General in a letter of 7th March 2014.

1.3. As will be apparent from the Terms of Reference and the Dáil Resolution, this Independent Inquiry and assessment or review has been directed to be carried out on an extra-statutory basis outside the legislative frameworks of the Acts authorising and governing tribunals of inquiry and investigations. It is a consequence of that non-statutory basis for the present Inquiry that it has not had competence to compel the production of documents or the giving of evidence. It has therefore been reliant upon the voluntary co-operation of the parties concerned and of those whom it has considered appropriate to approach.

1.4. It is a further consequence of the *ad hoc* and non-statutory basis of this Inquiry that the report has no authority to make binding findings of fact much less definitive findings adverse to the interests or reputations of individuals or undertakings implicated in the events or issues with which the report is concerned. It has not had authority to adjudicate on disputes of fact.

1.5. It must therefore be understood that as a result of those limitations, the conclusions presented in this report are based upon my personal evaluation and opinion as to the implications of the information available to me and the documentary and other evidence voluntarily provided to me. The report must not be read, understood or interpreted as constituting any judgment or definitive determination which allocates culpability, responsibility or liability.

1.6. The Ombudsman Commission is referred to in this report as 'GSOC' or 'the Commission'. References to "the Minister" and to "the Commissioner" are to the Minister for Justice and Equality and to the Commissioner of the Garda Síochána respectively; and references to "the Act" are to the Garda Síochána Act 2005, (as amended), except where otherwise stated.

1.7. The report is structured as follows; the Terms of Reference and the background and context to the Inquiry are first set out. It then summarises the contents of the reports on the detected sources of the suspected security breaches and the report commenting upon them as the basis upon which the Inquiry was directed. The relevant provisions of the Act are summarised in Chapter 7.

1.8. In Chapter 9 there is set out a summary of the evidence, both documentary and oral given and the information gleaned by me in the context of the Inquiry. There then follows my assessment and review of that material in accordance with paragraph 3 of

the Terms of Reference. In the final chapter my recommendations are given as invited by paragraphs 4 and 5 of the Terms of Reference. The appendices include a glossary of some of the technical terms used in the reports and evidence.

## 2. Terms of Reference

The Terms of Reference of the Inquiry were as follows:

1. *To establish a chronology and identify the sequence of events and facts leading up to and relating to the Public Interest Investigation pertaining to security concerns commenced by the Garda Síochána Ombudsman Committee pursuant to Section 102 (4) of the Garda Síochána Act 2005 on or about the 8th October 2013.*

2. *To examine all reports, transcripts, records, minutes, correspondence and documentation and consider any oral or other evidence as is deemed relevant to the aforementioned Public Interest Investigation.*

3. *To review and assess any evidence of a security breach or attempted security breach at the GSOC as informed by, inter alia, the chronology and facts established at (1) above or arising from the examination at (2) above, and as may have occurred at any time up to 18th February 2014.*

4. *If appropriate, to make recommendations regarding measures to improve the existing security arrangements of GSOC for the purpose of addressing risks to data and communications identified in the course of this review and to ensure the integrity and security of their data and information in the interests of maintaining public confidence in the ability of GSOC to discharge its statutory functions in the public interest.*

5. *To make any other recommendations, whether in regard to legislation or otherwise, as may be considered appropriate arising from the review aforesaid into this matter.*

6. *To report on the above matters within eight weeks or as soon as may be thereafter.*

## 3. Background to the Inquiry

The immediate background to the establishment of the Inquiry was this.

3.1. On 9th February 2014 an article appeared in a weekend newspaper under the heading "GSOC Under Hi-Tech Surveillance" asserting that the offices of GOSC had been *"targeted as part of a sophisticated surveillance operation which used 'Government-level technology' to hack into its e-mails, Wi-Fi and phone systems."* The newspaper in question was the Irish edition of the British weekly newspaper "The Sunday Times" published by the News Corporation Group. (The content of this article is

referred to in more detail at Chapter 12 below and a copy of the full text is attached as Appendix V).

3.2. In the light of the further information that has become available in the course of this Inquiry and is set out later in this report, it is notable that a number of specific statements of fact which were asserted in that article caused particular concern:

- GSOC was targeted in a sophisticated surveillance operation which used "Government level technology" to hack into e-mails, Wi-Fi and phone systems;
- A speaker phone in GSOC was "bugged" and the phone line was used to eavesdrop on meetings;
- GSOC's Wi-Fi network had been compromised to steal e-mails, data, confidential reports and possibly to eavesdrop on mobile phone calls;
- A second Wi-Fi system had been created to harvest GSOC data using an IP address in Britain;
- A device worked off GSOC's broadband network was compromised but wiped of all data by those involved as a "black operation."

3.3. The publication of this article and the assertions of fact which it contained provoked understandable controversy which required GSOC to give an explanation by way of briefing to the Minister leading in turn to the Minister's address to Dáil Eireann on 11th February 2014 and the appearance of the Commission members at a hearing of the Joint Committee on Public Service Oversight and Petitions ("PSOP") on 12th February 2014. In view of the existence of other controversies which have arisen during the period before or immediately after the establishment of this Inquiry, it is important to emphasise that this report is concerned only with the subject matter of paragraph 1 of the Terms of Reference namely the facts relating to the Public Interest Investigation commenced on 8th October 2913. (To avoid confusion with other GSOC investigations mentioned below, this subject investigation is referred to as "the P.I. Investigation").

3.4. The controversy has its origins in a security sweep or survey commissioned by GSOC from the British firm of counter-surveillance experts Verrimus Limited in September 2013. As a result of the initial engagement and surveys carried out by this firm and its subsequent re-engagement for the purpose of further tests, three written reports were furnished to the Commission. These were:

- A Technical Surveillance Counter Measures Survey Report dated 26th September 2013 covering the initial visit and sweep of GSOC offices (The "TSCM" Report);
- A supplementary report dated 29th October 2013 covering the tests and results of a subsequent visit on 19th and 20th October 2013; and (the "CC1/002 Report")
- An expert opinion on a forensic examination of two particular items of equipment carried out on behalf of Verrimus by KJB Forensics Ltd dated 16th December 2013 (the "[redacted] Report").

3.5. Following the eruption of the controversy, a second opinion by way of review of the contents of the three above reports was commissioned by the Minister from the firm Rits, an Irish specialist firm in counter-surveillance measures. This report raised doubts as to the tenability of the assertions made and conclusions reached in the advices given by Verrimus Ltd. In essence, doubt was expressed as to the validity of

the assertion made in the Sunday Times article that a sophisticated surveillance operation using government-level technology to hack into e-mails, Wi-Fi and phone systems had in fact been carried out and it advised that there were possible alternative and benign explanations for the "anomalies" identified in the Verrimus reports.

## 4. The Sequence of Events

4.1. The chronology and sequence of events relating to the P.I. investigation as called for by paragraph 1 of the Terms of Reference are set out in Appendix I to this report and should be read in conjunction with the summary of the evidence and information which follows.

## 5. Conduct of the Inquiry

5.1. For the purpose of this Inquiry I have sought and been provided with the documentation relevant to paragraph 2 of the above Terms of Reference by both the Department of Justice and Equality and GSOC.

5.2. In addition, I have had voluntarily provided to me documentation from Verrimus Ltd. To all of the undertakings and personnel concerned, I have underlined the voluntary non-statutory nature of this Inquiry and the absence of compellability.

5.3. Immediately upon taking up the appointment I met informally with the three members of the Commission to discuss with them the scope and objective of the Inquiry and to outline how I proposed to conduct it. The Commissioners showed me the rooms and equipment which had been in the subject of the Verrimus Survey. The Commissioners expressed their desire and willingness to co-operate as fully as possible but also their serious concerns as to their ability or entitlement to provide information and documentation having regard to the duties of secrecy or confidentiality which bound GSOC under the Act.

5.4. On 12th March 2014 I wrote to the Commission making a formal request to be provided with the materials listed in paragraph 2 of the Terms of Reference and furnishing a list of questions and points requiring clarification based on my reading of the materials already available to me. On 19th May 2014 I again met with the Commissioners and their legal representatives in order to invite them to clarify some points that had arisen during the Inquiry and to afford to them the opportunity that the legal representatives claimed as their entitlement to comment upon the conclusions to be expressed in this report. (See paragraph 9.78 *et seq.*)

5.5. GSOC chose to nominate a partner in the law firm Arthur Cox as its point of contact with me for this Inquiry. Arthur Cox for this purpose instructed Mr Felix McEnroy, Senior Counsel. Solicitor and counsel assisted the GSOC representatives and the Verrimus expert in preparing statements and volumes of exhibits which were furnished to me. Solicitor and counsel attended at the interviews of the GSOC officers and the Verrimus expert.

5.6. In agreeing to provide the Inquiry with the documents covered by paragraph 2 of the Terms of Reference, the legal representatives sought to define conditions upon which that would be done in order to accommodate GSOC's continuing obligations in

relation to sensitive and confidential contents of documents. Following an exchange of correspondence it was agreed that relevant documentation regarded as confidential would be collated separately and made available to be consulted by me in a room at the GSOC offices. The responses to my letter of 12th March 2014 were provided to me on 27th March 2014 and the documents regarded as sensitive, confidential or privileged were made available to me at GSOC on 19th April 2014.

5.7. It is appropriate also to record that both by submissions by counsel during interviews and in correspondence from Arthur Cox, GSOC maintained that there was a failure in the conduct of the Inquiry to apply the principle of fair procedures. It was asserted that both GSOC and Verrimus Ltd as GSOC's 'servant or agent' were entitled to be furnished with details of all evidence, advice and information available to or obtained by the Inquiry on which any 'finding' or recommendation in this report might be based. Although later modified, a letter of 28th May 2014 insisted that the 'draft findings' be furnished to Verrimus Ltd although Arthur Cox disavowed being the legal representative of that company and no such request was made by the company itself. By letter of 20th May 2014 as this report was being finalised, the legal representatives asked that I reconsider my "decision not to permit fair procedures". The argument was again advanced in a letter from the firm on 29th May 2014 in which as mentioned below, asserted that the principle of fair procedures entitled GSOC to be advised for prior comment of "*the material that grounded"* any proposed recommendation in response to paragraph 5 of the Terms of Reference.

5.8. These propositions were not accepted by me. I pointed out to the legal representatives that they had been present on behalf of their client throughout the interviews of the investigating officers, of the Verrimus expert, and of the Commissioners; that the Arthur Cox partner had attended the meeting with the principal of the firm that serviced the AMX system as mentioned in paragraph 9.71 below and that transcripts of the interviews had been provided to them. Any relevant information supplied to me by the various third parties mentioned below and any issues or possible explanations drawn to my attention by my own consultant or which occurred to me in considering documents or evidence, had been raised by me either during the interviews or in letters written to Arthur Cox for that purpose. I am satisfied that, commensurate with the objectives and limited outcomes of a non-statutory inquiry, due application has been given to the entitlement to fair procedures.

5.9. While the work done in compiling witness statements and assembling documentation was helpful in reducing the interview times required, the correspondence exchanged in dealing with conditions, objections and queries raised on behalf of GSOC and of Verrimus as its 'servant or agent' militated against conducting the Inquiry within the time envisaged in paragraph 6 of the Terms of Reference. That time-scale was however prescribed before it was known that GSOC would be simultaneously required to cooperate with two Inquiries.

5.10. I have, as mentioned, conducted interviews with the Commissioners of GSOC and also interviewed the authors of the Verrimus and Rits Reports. I have also had the benefit of technical advice from BH Consultants, an Irish consultancy firm specialised in information and communications security. In addition as described below, I have made enquiries of and been provided with relevant information by Bitbuzz Ltd whose Wi-Fi hotspot was identified in the sweep. The mobile phone service provider whose

UK country/network code featured in one detection also provided information. I also had the benefit of discussing with the principal of the firm which had carried out servicing and repairs to the AMX audio/visual system since 2011 the works recorded in their job sheets and service records as described in paragraph 9.71 below.

5.11. I was written to by the former Minister Deputy Alan Shatter who confirmed his availability to be interviewed in the event I had any questions in relation to his exchanges with GSOC or contribution to the Oireachtas proceedings in the period between the publication of the Sunday Times article and the establishment of this Inquiry. I thanked him for his letter and informed him that while I had read the correspondence, transcripts and memoranda which had been furnished to me in that respect, I did not consider that any issues relevant to the Terms of Reference arose from them which would call for questions to be put to him by me.

5.12. Office accommodation and secretarial equipment was provided to the Inquiry by the Office of Public Works and part-time secretarial and stenographic support was retained by me as required.

5.13. I wish to record my grateful appreciation for the skilled work carried out for me by Ms Siobhán Murphy and Ms Deirdre O'Malley in providing secretarial and stenography support to the Inquiry and the preparation of this report for presentation.

## 6. Pre-Inquiry Technical Reports

The Verrimus Reports

6.1. As already indicated, between 23rd September and 16th December 2013, this UK specialist firm delivered three reports on the work it had carried out for GSOC and a commentary on these reports had been furnished to the Minister by the Rits firm. The contents of these documents can be summarised as follows.

The TSCM Survey Report

6.2. This report covers the work carried out by operatives of Verrimus over 28 hours during the period of 4 days 23rd – 27th September 2013. The work was carried out on each day between 7.00 p.m. in the evening and 3.00 a.m. the following morning. The purpose of the survey was described in the report as being *"to identify any current technical surveillance threats and to identify vulnerable areas of critical information defence due to a perceived threat and quantifiable evidence of a verbal indicator of eavesdropping in one of four known areas."* The relevant offices of GSOC were *"surveyed for current and historic signs of CAT A-E threats using technical, physical search and hostile attack simulation methods."* The report details twelve particular surveys that were conducted:

1. Full radio frequency signal search and spectrum analysis 10KHZ-26GH
2. Full Wi-Fi threat detection survey
3. Full thermal emission spectral analysis
4. Full active GSM survey, all networks
5. Full mains sub-carrier scan
6. Full Non-Linear Junction detection search (2500MHZ) 4 Wattcw

7. Full strip down of all IT ancillaries
8. Full telephone line analysis
9. Full physical domain search
10. Pin-point direction finding of all localised transmissions
11. Full data network frequency domain reflectometry
12. Full forensic light survey, multiple wavelengths.

6.3. In all but three of those surveys the report found "No Threat Detected." The three surveys in which threats were detected were those itemised at 2, 8 and 9 above and these were described at the top of the report as "**Red Flag Warnings**" as follows:

- 2 Full Wi-Fi threat detection survey – **Multiple Threats Detected**
- 8 Full telephone line analysis – **Threat Detected**
- 9 Full physical domain search – **Threat Detected.**

The report then gives further detail of the results of those surveys and searches as follows.

<u>The Full Wi-Fi Threat Detection Survey</u>

6.4. Under this heading, it was reported that during the wireless network analysis in the area of the GSOC boardroom, an insecure wireless local access network was detected. This is further detailed as follows:

> *"The network access point named AMX (...) was located to the conferencing system in the boardroom. This access point has wired equivalent privacy (WEP) access security. WEP is a security algorithm for IEEE 802.11 wireless networks, introduced in 1999 and has been superseded twice making it virtually obsolete since 2004."*

6.5. The author of the report then expresses the opinion that the WEP security in question is considered wholly insecure and easily hacked even by an untrained individual with free software and instructions found on the Internet. Once a WEP access point has been accessed, it is possible for a hacker to access, control and intercept any device or data on that network. The significance of this opinion is then illustrated by two diagrams which contrast a secured WLAN (i.e. a wireless local access network) and an insecure WLAN.

6.6. The protection afforded by a white noise generation system in the boardroom was also considered inadequate and the operatives conducting the surveys arranged a hostile attack simulation by recording audio from the room on a simple device. (See paragraph 6.14 below.) This achieved a recording both inside the room and from the wall quite easily. The view is expressed: *"The ramifications (sic) of this is that any conversation ever held in this area has not been secure."* The view is then expressed that if this area of vulnerability is taken in conjunction with the possibility that unauthorised access to the conference microphones in the room could be obtained via the insecure access point identified above, *"an attacker could have unrestricted audio feed in this room as and when required."*

6.7. Under this Full Wi-Fi Threat Detection Survey, a wireless device was also identified as vulnerable. This consisted of the identification of a media access control MAC address (see Appendix II) detected in the boardroom area and described as having *"... 100% been attached to the AMX conferencing wireless system and the open public Wi-Fi, Bitbuzz outside the building. ... If the device is an authorised part of the organisation's network it should never have been attached to an external present open public Wi-Fi network. If this device is not an authorised part of the organisation's network it should never have been attached to the organisation's network."*

6.8. It is to be noted however that at that stage, the operatives conducting the survey did not know whether this particular device was in fact part of any authorised network within GSOC. The report concludes this section with the reservation:

> *"The team had insufficient time and information (no organisational network diagram) to pinpoint the location of the device. Power readings localised the device to the boardroom area."*

6.9. In other words, although the scan or survey picked up and identified the MAC address of a wireless device in the area of the boardroom in apparent contact with a public open Wi-Fi network, the particular device emitting the signal was not located at that stage.

<u>The Full Telephone Line Analysis</u>

6.10. The second survey which identified a threat was that of the "Full Telephone line analysis." This concerned a "Polycom unit" located in the office of the GSOC Chairperson. In practical terms this is a telephone receiver unit with a dialling keypad but without a handset used for holding conference calls; that is to say, telephone conversations in which a number of callers both inside and outside the building participate simultaneously.

6.11. This Polycom unit was subjected to a number of tests to determine whether or not it was compromised or "tapped". The last test to be conducted is described as an "alerting test" and is the final one conducted because its effect is to alert any covert eavesdropper to the fact that the surveillance of the line has been detected. An audio signal (in this case music) is sent down the line and will be heard by an eavesdropper monitoring the line. This alert test was carried out at 01.45 hours and the report describes what then happened:

> *"The test device was still connected and neither operator was touching the device. The device received a call in of around three rings' duration. Meaning a person must have made a call to the device direct, as the organisation's switchboard was on out-of-hours service."*

6.12. The report then contains the following assessment:

> *"The likelihood of a 'wrong number' at that time to that exact unknown number at the time of an alerting test is so small it is gauged at virtually zero."*

6.13. The Verrimus expert expressed the view that the audio test:

> "*May have triggered a response form an Attacker/Listening Post/Monitoring station. Likely that the 'listener' found the intermittent audio input (music) on the line at 01.40 hours an odd occurrence and without thought or consideration to the possibility of a TSCM operation decided to test the call line to ensure it was working. Assuming there would be nobody there at that time."*

Physical Domain Search

6.14. The third threat detected was that from the "Full Physical Domain Search." Although that term is not used elsewhere in this report, the author confirmed in evidence to the Inquiry that this referred to the vulnerability identified at paragraph 1.4.2 of the report namely, the ineffectiveness of the Research Electronics International (REI) white noise generation system ANG-2000 which had been installed in the boardroom area (see paragraph 6.6 above). This was intended to create a perimeter of noise around that area to defeat eavesdropping by concealed microphones, audio transmitters or other devices. This was judged to be ineffective as shown by the simulated hostile attack referred to above.

6.15. The report also pointed out that the offices are overlooked from close locations and vulnerable to surveillance by video recorder with telephoto zoom which could record lip movements of conversations for later forensic reading as well as password and user-name inputs on IT systems and screen documents. It comments: *"Vulnerability to this type of attack is assessed as **Very High** falling to low if window coverings are kept closed."*

6.16. The report notes that GSOC had an insecure network and the possibility that unauthorised wireless network devices were in place. *"The vulnerability to his type of attack is assessed as **Very High falling to Low** if the network is secured and only authorised devices are allo**we**d into the building."*

The CCI-002 Report

6.17. This brief three page document covers the work carried out by Verrimus during the follow-up visits to the GSOC offices on 19th and 20th October 2013. It is described as supplementary to a "*full evidential log of events and imagery*" which was maintained and signed at the time. It is also notable that this report proceeds on the basis of an assumption which is stated under the heading "Threat" at the outset. *"It is assumed from the brief that any attack in the areas of concern (AOC) would be up to intelligence service attack level."* The apparent objectives of the task were stated:

> *"Client requests:*
> *1. Locate client '4B';*
> *2. Inspect Comms Units;*
> *3. Trace wiring from Comms Unit."*

6.18. Four particular tasks were undertaken, two of which disclosed no threat or abnormality. These were the inspection of the "Coms Unit" and the tracing of all wiring from that unit. (The "Coms Unit" is a bank or stack of consoles housing the

communications equipment in the boardroom and located behind a door in an alcove on an outside wall of that room.)

6.19. The wireless device with the MAC address which had not been located during the September surveys was located and identified as an AMX wireless pad in the Media Room of the offices. This is then referred to as "Device 4B" based on the last two digits of its MAC address. This unit was monitored over two days during the survey and was again found to connect itself to an insecure external Wi-Fi (Bitbuzz) network on numerous occasions.

6.20. The second abnormality detected on this occasion was new and was described as a "fake GSM/3G base station" detected in the area. This base station broadcast a mobile MCC/MNC identifier[1] allocated to a UK mobile phone service provider which was not genuine in Ireland. The significance of this detection is then described as follows:

> *"This is good evidence of a localised intelligence-gathering or interception device. Symptomatic of something in the nature of a dedicated 3G IMSI grabber or interceptor, targeting UK mobile phone(s) on 3G."*

6.21. Images were then included to show the UK spoofed network present at that location and a screen shot of the mobile phone handset which picked up the UK network signal.

6.22. (It is perhaps unnecessary to explain that when in use a mobile phone will emit a signal which searches for the nearest or strongest mast or base station of the mobile phone network to which the user subscribes. A call made will then be transmitted via that connection and will continue to be routed to further base stations of that network if the user is moving around. The significance of the abnormality identified in the report is that a source appeared to be detected which was falsely mimicking a 3G UK network and thus possibly attracting subscribers to that network making calls within its range to connect to it rather than connecting as a roaming call through a local Irish network.)

6.23. It is to be noted that although the TSCM Report refers to *"a perceived threat"* and to *"quantifiable evidence … of eavesdropping"* and that the CC1/002 Report refers to an attack being *"up to Intelligence Service attack level",* neither report contained any express finding to the effect that any such attack was actually taking place or had in fact taken place. Those references in the reports were, as explained later below, based upon information furnished to the Verrimus operatives by GSOC officers.

6.24. A conclusion is given as follows:

> *"All objectives were met.*
> *Further to objective: evidence of 4B acting in an insecure manner was evidenced and a fake or spoofed 3G base station was detected locally."*

<u>Third Report: KJB Computer Forensics</u>

[1] See Appendix II

6.25. The third report is that of [redacted] of the above firm which had been engaged by Verrimus to conduct a forensic examination of the two Wi-Fi devices which were the subject of the two earlier reports. Mr [redacted] visited the GSOC offices on 19th November 2013 on the occasion of the "special operation" described below following which he examined the two devices which he refers to respectively as "Device 4B"and "Device BC". Each is an AMX Modero Viewpoint (MVP) Wireless Touch Panel. (In layman's terms, these are touch panel remote controls inter-connected wirelessly to the audio and video equipment used as typical conference room equipment for screen presentations and which enable connections to be made between projector, microphones, laptops and the display screen. A detailed description is given in the manufacturer's user documents in Appendix IV).

6.26. It is notable that Mr [redacted]'s work proceeded on the basis that it had been explained to him, *"That one of the touch panel devices had been the target of an unauthorised wireless network attack… associated with Bitbuzz a wireless hotspot provider located in the UK and Ireland."*

6.27. Mr [redacted] later disassembled the two devices. Each was fitted with a 64mb compact flash card and a wireless network card. The former stores the device's operating system and configuration files. The examination of the two devices involved forensically imaging or copying the flash drives installed on each panel using a computer program which sequentially reads through the entire storage space on the disk and writes that data on to a suitable target namely, a large computer network volume.

6.28. In examining Device 4B, Mr [redacted] noted that the wireless adapter should have displayed the manufacturer's details. He remarked, *"The absence of these details infers the device has been disassembled prior to our investigation commencing."* This was not the case with Device BC which appeared to retain the original components.

6.29. Mr [redacted] conducted a series of keyword searches for references to "Bitbuzz" fragments or the entire word but found no such references in any shape or form. He examined both devices for traces of a "malware attack" but found nothing to indicate that malicious software had been installed on either device. He did however note an anomaly with *"the last accessed dates and times associated with files and folders on both devices"*. On the last three dates on each, two were common but on Device 4B the date 6th December 2006 did not correspond with date 18th August 2006 found on Device BC. The author observed:

> *"Clearly the system date and time has been adjusted either manually or as a result of a system up-date. What is not clear is why there is three separate dates; the files associated with the date 1 Jan 70 are predominantly system files, if there was a system up-date these should have dates associated with the date and time of up-date. There are a number of possible explanations for the discrepancies with the other two dates; this may be worth further investigation with the client."*

6.30. He then summarised his results and opinion as follows:

> *"My examination revealed the security and network configuration of both devices but did not reveal the presence of any references to 'Bitbuzz', wireless hotspot.*

*Whilst there were anomalies with some of the dates and times associated with files/folders on both devices, there was no other evidence to suggest malicious software had been successfully loaded on either device."*

6.31. In the light of the further information obtained about Device 4B and given later in this report, it is relevant to note that the [redacted] forensic examination of the device appears to have been confined to examining whether the flash card retained any evidence of communications with the Bitbuzz hotspot. It was not concerned to consider its microphone capability or to examine whether there was any link between the substitution of the replacement components and its reconfiguration for connection to the hotspot.

Expert Opinion of Rits

6.32. The fourth technical assessment which had come to hand prior to the establishment of this Inquiry is the report commissioned by the Minister from the firm Rits Information Security. The report is, in effect, a review of the three above reports and opinions and not a separately-conducted forensic examination of the items of equipment or the location involved.

6.33. The Rits Report gives its opinion on a series of specific aspects of the Verrimus work and its main conclusions can be summarised as follows:

- Based solely upon the contents of the three Verrimus documents, there was no evidence that any technical or electronic surveillance of GSOC had taken place. It is considered probable that there are alternative and benign explanations for the anomalies identified in the three reports.

- It is pointed out in relation to the description of the insecure WLAN (diagram 2 in the TSCM Report (see para 6.5 above) that the AMX system in question is not fact connected to any internal GSOC network.

- The reports do not contain any evidence that Device 4B had been the target of any actual attack associated with the Bitbuzz Wi-Fi network.

- Contrary to the "Red Flag Warning" in respect of the Full Wi-Fi Threat Detection Survey, there is in fact no connection between the wireless network for the audio/video remote controls of the conference equipment and the wired network of GSOC's file services and databases. No user of the Wi-Fi network in question could obtain access to those servers.

- No detailed analysis of any network traffic between the AMX device and the Bitbuzz network appears to have been undertaken.

- In relation to the call-back anomaly occurring on the Polycom Unit, the following points are made:

    a) No in-coming caller ID (either displayed or unknown) appears to have been noted on the operatives' test device;

b) The Polycom Unit was connected by analogue circuit to the GSOC exchange or switchboard (a Nortel Digital PBX or private branch exchange). It is considered possible that the alert test conducted might have caused the PBX to react by performing an automatic call-back to reconfigure, reset or re-initialise the analogue port;

c) The telephony connection for GSOC is provided through the Government networks which is a digital service connected to the PBX. There is no physical analogue circuit which connects the Polycom Unit to an external telecom carrier network so that an in-coming external call would have to have been routed through the digital service of the PBX.

- The Fake UK 3G Network: It is considered that there are a number of possible explanations for the country/network code of the 3G UK network other than that of a dedicated 3G IMSI grabber or interceptor. First, 3G UK network like other mobile operators provides devices (femtocells) to subscribers for mobile coverage in areas where the signal is weak. It is not unknown that customers sometimes take these devices abroad and connect them to an internet connection in order to avoid roaming charges. The possibility that this is what occurred here had not been investigated.

- It notes that there are a number of Wi-Fi networks in the vicinity of the GSOC premises which would indicate the presence of a workshop or laboratory where GSM and related technologies are being worked upon. The possibility is raised that a customer might have brought a 3G UK femtocell from the relevant network for repair which would then display the 3G UK network identifier if powered on and connected to the internet.

- The opinion also questions the description of the 3G IMSI grabber or interceptor as a device available only at "Government agency level." It states that perfectly legal and off-the-shelf software and hardware which can perform these functions are available at a cost in the region of €5,000. It also points out that no further tests appear to have been carried out to ascertain whether the supposed IMSI catcher disabled the encryption applied to calls made through that device.

- Finally, it is pointed out that an IMSI catcher device can have a range of up to several kilometres depending upon the level of power applied to its antennae. Thus, even if there was an IMSI catcher detected in the area of the GSOC offices, it does not necessarily follow that it was targeting communications in those offices.

## 7. The Garda Síochána Act 2005

7.1. GOSC is established under Part 3 of the Garda Síochána Act 2005 and its functions are set out in Section 67 of the Act in that Part. The functions of the Commission include receiving complaints made by members of the public concerning the conduct of members of the Garda Síochána and the carrying out of the duties and the exercise of the powers assigned to the Commission under Part 4 of the act in relation to such complaints. The functions also include a duty to report the results of investigations

under Part 4 to the Garda Commissioner and, where appropriate, to the Director of Public Prosecutions. In addition to receiving and investigating such complaints, the functions of the Commission include the conduct, in accordance with Section 102, of other investigations of matters concerning the conduct of members of the force.

Investigation of Complaints

7.2. Part 4 of the Act details the manner in which complaints can be made and received and the procedures to be followed when complaints are to be investigated by the Commission. A complaint may be made by a member of the public directly to the Commission or by making it to the Garda Commissioner; to any member of the force at a Garda Síochána station; or to a member at or above the rank of Chief Superintendent at a place other than a Garda station (Section 83). Section 84 provides for a time limit on the making of a complaint and Section 87 requires the Commission to first assess the admissibility of the complaint. When a complaint is determined to be admissible, Sections 88-94 prescribe the procedures by way of notification that are to be followed by the Commission in conducting its investigation of different types of complaint.

7.3. Investigations are carried out by the Commission through officers designated by it pursuant to Section 73 of the Act ("designated officers"). Subject to certain exceptions, the investigative functions of the Commission under Part 4 may be delegated by the Chairperson to its members or officers including therefore an investigation under Section 102(4). (Section 75(1)).

7.4. In addition to the investigation of admissible complaints received or made in those ways, Section 102 of the Act empowers the Commission to conduct other types of investigation in particular circumstances. Under sub-section (1) the Garda Commissioner must refer to the Commission "*any matter that appears to the Garda Commissioner to indicate that the conduct of a member of An Garda Síochána may have resulted in the death or, or serious harm to, a person.*"

7.5. The scheme of the Act, therefore, is that investigations to be undertaken by the Commission originate mainly in an admissible complaint received from or on behalf of a member of the public, either directly or through the channels prescribed in those sections, or in a reference from the Garda Commissioner.

Public Interest Investigations: Section 102

7.6. By way of addition to these complaint or reference-based procedures, the only basis upon which the Commission has competence to conduct any investigation entirely of its own initiative is that provided for in sub-section (4) as follows:

> *"The Ombudsman Commission may, if it appears to be desirable in the public interest to do so and without receiving a complaint, investigate any matter what appears to it to indicate that a member of the Garda Síochána may have (a) committed an offence or (b) behaved in a manner that would justify disciplinary proceedings."*

7.7. The only further manner in which such an investigation can come to be conducted by the Commission is that provided for in sub-section (5) where the Minister "*if he or she considers it desirable in the public interest to do so, may request the Ombudsman Commission to investigate any matter that appears to the Minister to indicate that a member of the Garda Síochána may have done anything referred to in sub-section and the Commission shall investigate the matter."* In other words, the Commission has a discretion, if it is of the opinion that it is in the public interest to do so, to investigate a matter under sub-section (4) of its own initiative and may also, without forming the necessary opinion, do so if the Minister has formed that opinion and so requests pursuant to subsection (5).

Reporting Results

7.8. Section 103(1) imposes on the Commission a duty to provide certain persons with sufficient information to keep them informed of the progress and results of an investigation under Part 4. If the investigation results from a complaint, the persons to be kept informed are the complainant, the member of the Garda Síochána whose conduct is the subject matter of the complaint, the Garda Commissioner and any other person that the Commission considers has a sufficient interest in the matter.

7.9. Where the investigation is one conducted pursuant to Section 102, those required to be kept informed are *"the member of the Garda Síochána whose conduct is the subject matter of the investigation"* together with the Garda Commissioner, the Minister and any other person that the Commission considers has a sufficient interest in the matter. Thus, irrespective of the outcome, the result of any completed investigation under S. 102(4) is required to be reported by the Commission to, *inter alia*, the Minister and the Commissioner.

7.10. It is to be noted, accordingly, that in the case of the only investigation which the Commission can commence on its own initiative, the objective of the investigation is to ascertain whether a member of the Garda Síochána may have committed an offence or misbehaved in a manner that would justify disciplinary proceedings and the fact that the member in question is required to be kept informed of the progress and results of the investigation would seem to suggest that the matters available to the Commission by way of indication in that regard, concern some identified or potentially identifiable member of the force.

7.11. It is obviously possible to conceive of a situation in which an event has occurred or circumstances have arisen which can only have occurred or arisen as the result of an offence or misbehaviour on the part of one or more members of the Garda Síochána but whose identities are unknown. In such a situation the power to initiate a sub-section (4) investigation may be exercisable. In my opinion, however, it is possible that the sub-section would be construed by a court as confining the exercise of this power to cases where the indicative matters before the Commission provide a substantive basis for implicating some member or members of the force and therefore as excluding cases where the matters in question may be attributable to other persons and where there is no necessary implication of an offence or misbehaviour on the part of any member of the force either alone or jointly with other non-member third parties.

7.12. It is appropriate to record however that when I mentioned this possible lack of clarity in the wording of S.102 (4) to the Commissioners in interview on 19th May 2014 they strongly disagreed. (See paragraphs 9.19 and 9.83 below). They took the view that the threshold for the exercise of this discretion was low and they considered that the Commission was intended to be entitled to have recourse to the sub-section in any case where the possibility existed that the subject matter was potentially attributable to the misbehaviour of a member of the Garda Síochána whether identified or not and whether or not other parties not members of the force were also implicated. They referred to an investigation of a complaint which resulted in the conviction of two individuals one of whom was a garda and the other a member of the public.

Powers of Investigation

7.13. Finally, it is to be noted that where the Commission directs the initiation of a statutory investigation, the designated officers charged with conducting it are endowed with the powers privileges and immunities listed in Section 98(1) as well as all powers conferred upon any member of the Garda Síochána under legislation or at common law. The former include powers of entry, of search and of arrest without warrant and detention for questioning. Section 101(1) requires that on completing an investigation under S. 98 the designated officer concerned is to report its results to the Commission. The provisions of Section 98 apply to a public interest investigation under Section 102(4) by virtue of Section (6) of the latter section.

## 8. The Section 102(4) Investigation of 8th October 2013

8.1. The direction to commence a Public Interest Investigation under Section 102(4) of the Act was given by GSOC's Acting Director of Investigations and took the form of a hand-written document signed by him. Having referred to the two threats identified in the TSCM Survey Report from Verrimus, he stated:

> *"I am of the opinion that, to the extent these threats can be proven, Section 102(4) of the Garda Síochána Act 2005 engages. That is to say, that such surveillance may have originated with the Garda Síochána and if so, a member of the Garda Síochána may have committed an offence or behaved in a manner that would justify disciplinary proceedings. I am further of the opinion that it is desirable in the public interest that the matter be investigated to ensure that the objectives of the Ombudsman Commission as set out in Section 67(1) are not compromised or impugned. I have discussed the matter with the Chairperson Mr Simon O'Brien today Tuesday 8th October 2013 and he is in agreement."*

## 9. Evidence to the Inquiry

The GSOC Officers

9.1. Evidence was given to the Inquiry by the three designated officers who were mainly responsible for the decision to commence the P.I. Investigation and for its conduct. They were also the principal members of the Commission personnel who had been involved in the events described in 2012 and the first half of 2013 which contributed to the atmosphere of tension and distrust between the Commission and the Garda Síochána. (In view of their roles in other investigations by GSOC, the officers will be referred to as Officers A, B[2] and C respectively).

9.2. In explaining their understanding as to why the P.I. Investigation came to be directed, these officers described and explained the pressure they had been under and the atmosphere of anxiety and tension that came to exist within the Commission during the latter half of 2012 and the first half of 2013 as a result of what they saw as a

[2] Officer B was Deputy Director of Investigations and was Acting Director until November 2013 when a vacancy for the senior post was filled.

serious deterioration in relations with the Garda Síochána and particularly with officers at the most senior level in the force. This aspect of the background has been referred to by the Chairperson of the Commission at the hearing before the PSOP Committee on 12th February 2014.

9.3. It is unnecessary to go into the details of the operational matters which brought about this situation. The principal elements can be summarised in general terms as follows. There had been protracted and difficult negotiations in an attempt to agree revised protocols for the purposes of Section 108 of the Act since before the appointment of the new Commission in December 2011. Of particular difficulty in those negotiations were issues in relation to the timeliness in the provision of requested information from Garda Síochána and related matters of co-operation between GSOC and the force. The topic of serious delays which had been encountered in the provision of such information was referred to in GSOC's Annual Report for 2011 published in June 2012. This problem of adherence to the existing protocols was also raised in the Annual Report for 2012 published by GSOC in May 2013.

9.4. The problem encountered in obtaining requested information from the Garda Síochána appears to have crystallised or become more acute in the context of two particular and protracted statutory investigations which were under way by GOSC for a number of years prior to 2013 and which were of considerable importance and sensitivity. In accordance with Section 103 of the Act, GSOC's report on the first of those investigations was sent to the Minister and the Garda Commissioner in the first week of May 2013. In December 2012 GSOC had sent a file arising from one of those investigations to the DPP to consider a prosecution. In April 2013 the DPP directed that no prosecution be brought.

9.5. During this period the Commission also became extremely concerned that a number of articles had appeared in newspapers relating to these investigations of which the contents suggested that confidential information in relation to them was being leaked to the media.

9.6. Throughout this period and in relation to the two important investigations, the GSOC officers complained of encountering delay, obstruction and refusals on the part of senior gardaí in the provision of requested information and access to documents or other evidence. One of the officers characterised the general attitude adopted by senior gardaí towards the Commission by reference to a remark made by one member of the force: *"We'll tell you what you can get and when you can get it."*

9.7. More specifically, during the period when the officers were engaged in writing the final reports on the investigations for the purpose of Section 103 of the Act, two of them came to suspect that they were the targets of "ambient listening." (See Appendix II). They found that the mobile phones which they used constantly in their contacts with Crime and Security Branch of the Garda Síochána began to run down very quickly. Although fully charged overnight and normally good for heavy use over 24 hours, they would be depleted within 2 hours or less without there being any change in use. They considered this to be possible evidence that their mobile phones had been interfered with. They stated that since the suspected surveillance had ceased, those same phones and batteries had resumed normal performance.

9.8. One further incident was referred to as something that contributed to the sense of suspicion that the GSOC officers were the target of surveillance. In July 2013 a meeting between the GSOC Chairperson and the Garda Commissioner had been scheduled to take place. A few days prior to the meeting the Chairperson and the designated officers met to discuss, amongst other subjects, the Commission's report on one of the above investigations under Section 103; a special report which had been submitted by GSOC to the Minister pursuant to Section 80 (5); the continuing negotiations on the protocols and the general problem of timeliness in the provision of requested information. In the course of that discussion someone suggested the possible use of a particular phrase to describe one of the activities involved in the investigation. It was agreed that the expression should not be used. When the Chairperson reported back after the meeting with the Commissioner, surprise was expressed that although the phrase in question was not used by the Chairperson, it was used by someone on the Commissioner's side of the delegation.

9.9. It was confirmed in evidence to this Inquiry that one of the issues in the earlier investigation related to the handling of informants. The expression discussed as apt to describe that issue was *"running an informant on or off the books"*. It might be thought that such an expression was probably one which would occur to an officer in any English-speaking police force to describe the particular activity, but its use in these circumstances nevertheless appears to have contributed to the heightened suspicion of the designated officers. Indeed, Commissioner Fitzgerald had used the expression on the occasion of the earlier presentation by GSOC to the PSOP Committee on 3rd July 2013.

9.10. The officers said that it was at this point namely, mid-July 2013, that it was decided to proceed with carrying out a counter-surveillance sweep of the offices which had previously been mooted but had not been followed up.

9.11. One of the designated officers was asked to undertake discreet enquiries as to which specialist firm might be appropriate to carry out the sweep. It was quickly discovered that the firm which had conducted the original sweep of the building in 2007 was no longer available. Following enquiries with the equivalent UK authority, the IPCC, contact was made with the firm Verrimus Ltd and Officer A got in touch with Mr [redacted] of that firm by phone call and text message. For this purpose Officer A purchased a supermarket "pay-as-you-go" mobile phone which was left unregistered so as to remain untraceable to him. In the initial briefing, the officer described to Mr [redacted] the incident mentioned above involving the use of a particular expression or phrase at the meeting with the Garda Commissioner but without repeating the actual expression. This appears to be the source of the reference in the TSCM Report to *"quantifiable evidence of a verbal indicator of eavesdropping."* The officer instructed Mr [redacted] that a security sweep was to be carried out in four particular areas of the GSOC offices. Shortly afterwards on 26th August 2013, Officer B asked Officer A to include two additional rooms, the Boardroom and the senior investigating officers' meeting room, in the areas to be covered by the sweep.

<u>The Verrimus Survey – 1st Visit</u>

9.12. As described at paragraph 6.2 above, two operatives from Verrimus conducted a counter-surveillance survey and tests at the GSOC offices between 23rd and 27th

September 2013 when the threats identified in the subsequent TSCM Report were detected. These included particularly Threat No. 1 – the wireless device in the Boardroom connecting itself to a Bitbuzz Wi-Fi network in the vicinity; and Threat No. 2 the possible interception of the conference call line on the Polycom unit in the office of the Chairperson.

9.13. At that point the officers did not know whether the Wi-Fi AMX network of the audio/video equipment was in any way connected to GSOC wired computer/server networks in the offices. This scan picked up the 12 digit MAC identifier address of some device which appeared to be connecting to the Bitbuzz network but the particular AMX device which was effecting the connection was not identified during the visit.

9.14. The TSCM Survey Report was received by GSOC officers on 7th October 2013.

9.15. Officer A and Officer B considered that the report had identified two potentially significant and serious intrusion threats. They discussed the implication of this development with the Chairperson on the morning of 8th October 2013 and it was agreed that a formal investigation was needed in order to examine the threats further and to ascertain their possible cause and sources.

9.16. It was agreed that a Public Interest Investigation under Section 102(4) of the Act was the appropriate mechanism for this purpose.

9.17. While the Chairperson had been thus briefed, the formal decision to exercise the power conferred by that sub-section was not taken by the Commission members as such. It was taken by the Acting Director of Investigations pursuant to the function which had been delegated to him since 2007 under Section 75 of the Act. The P.I. Investigation was thus commenced on 8th October 2013.

9.18. The Investigating Officers emphasised that, contrary to subsequent public comment, they had not at that point limited their suspicions as to the sources of the intrusions to members of the Garda Síochána. Officer B had considered a range of other parties who might possibly be responsible including organised criminal groups, possible uncontemplated persons or identities and, given the publicity that had attached to the phone hacking scandal in the United Kingdom, journalists.

9.19. Based on their understanding of the nature of the threats that had been detected and the recent fraught nature of relations with the Garda Síochána, however, they felt that eavesdropping or interception by one or more members of the force could not be ruled out. Officer B considered that, as he put it, Section 102(4) of the Act "was engaged" because there was a possibility that a member of the Garda Síochána might have thus committed an offence or breach of discipline. It was on that basis that he formed the opinion required for reliance upon Section 102(4). He explained that investigations had often been conducted into complaints even though a complainant had not named or identified any specific member of the force. He considered that this "low threshold" also applied under S. 102(4).

The Verrimus Survey – 2nd Visit

9.20. On 9th October 2013 arrangements were made to re-engage Verrimus to carry out further investigation and tests and a second visit by the operatives took place on Saturday 19th and Sunday 20th October 2013.

9.21. This work succeeded in identifying and locating the AMX device which was designated as "Device B4" as the MAC address of the AMX touch panel in question ended with the digits 4B. A second such device was designated "Device BC".

9.22. It was also established that the AMX audio/visual system was not in any way connected to any GSOC computers, servers or wired network. Monitoring of Device 4B did not disclose any connection with the Bitbuzz network during Saturday 19th October. On the following day, however, the device appeared to establish a live connection. As it was known that the Bitbuzz network in question was in a store/coffee shop on the ground floor of the same building, one of the Verrimus operatives was asked to go down and see if any person was there using a hand-held computer or mobile device. He reported back that there was one person there using such a device.

9.23. Officer A gave evidence that while this enquiry was being made, he noticed a white van parked in the street with a direct line of sight to the GSOC Boardroom. He went down to the store/coffee shop to see if he could identify the individual with the hand-held device but the person had left. He then walked past the white van which had windows which were blackened out. He walked around the block and saw two men walking together on three separate occasions. On the third occasion when the men saw him, they turned around and walked away. Based on his extensive experience of counter-surveillance, he considered this to be a possible indicator of a surveillance operation in the vicinity of GSOC at the time when Device 4B established its live connection to the Bitbuzz network on that day.

9.24. On the same day, as part of a routine test, available GSM mobile phone networks were searched for on an iPhone by one of the Verrimus operatives. This produced what was considered to be the unexpected result that in addition to the known local networks of the 5 digit country/mobile network code for a United Kingdom 3G mobile phone network was also displayed. This was subsequently identified as the code applicable to a 3G network in the United Kingdom which has a sister network in this country. The Verrimus operatives explained that this was "symptomatic of" the presence in the vicinity of a fake GSM/3G base station and therefore evidence of a localised intelligence-gathering or interception device known as an "IMSI catcher." (See Appendix II).

Verrimus Survey – 3rd Visit

9.25. Following the receipt of the CC1/002 Report on 29th October 2013, the officers decided to seek access to records of communications to the hotspot from Bitbuzz and of phone calls from Eircom and the necessary statutory authorisations were signed. A meeting with a representative took place on 24th October 2013 and the requested data which was confined to the period 19th to 21st October was supplied the following day. They also decided in conjunction with the Chairperson that in order to pursue the

investigation further, it was necessary to mount a special counter-surveillance operation with a view to drawing out the attackers and locating and seizing the IMSI catcher. For this purpose, a "legend" was prepared and agreed. This was a document setting out deliberately false and misleading information to the effect that serious errors had been made in a previous report of an investigation carried out by GSOC. It was considered that this false information would have been of particular interest to the suspected eavesdroppers. Accordingly, a meeting was arranged for the morning on Tuesday 19th November 2013 in the office of the Chairperson at which this information was to be discussed. The meeting was attended by the investigating officers and by two of the Commissioners. The Chairperson of the Commission participated from the United Kingdom by conference call conducted over the Polycom unit in his office. The two Verrimus operatives returned to Dublin on 18th and 19th November for the purpose of monitoring the detected threats during the meeting in order to detect, trace and, if possible, locate the fake GSM base station or IMSI catcher which had been detected at the previous visit. The investigating officers also arranged for officers to be available on stand-by to carry out arrests in the event that surveillance was discovered.

9.26. During the meeting lasting approximately one hour, the false information was discussed but no surveillance activity was detected. The monitoring continued until 16.00 hours on 19th November 2013 without any surveillance activity being detected.

9.27. On conclusion of the operation the two AMX control panels were disassembled by the Verrimus consultant engineer and forensically examined with the results described in the [redacted] Report.

9.28. Officer A who had considerable experience and expertise in intelligence techniques both with GSOC and agencies in other jurisdictions expressed the view that the forensic examination of the components of Device 4B was a distraction. It was not necessary to dismantle the device in order to reconfigure it. All that was needed was its password and having investigated it, he found that nobody in GSOC had it.

9.29. Although the point is not expressly made in the Verrimus reports, he explained what he understood to be the significance of the threat posed by the abnormal behaviour of Device 4B in connecting to the Bitbuzz hotspot. He confirmed that while that device did not contain a microphone the conference system did, *"So once you hack into the system you hack into all its functionality."*

9.30. He described what happened when it was monitored on 19th and 20th October 2013. There was no connecting activity observed on the Saturday or at first on the Sunday:

> *"But on Sunday we had the full team in place and we were monitoring again and initially it didn't connect. … More or less in around the time that the coffee shop opened it did connect and I can't remember the specifics, but it's all recorded and screenshots were taken of the displays as they occurred. It connected. And data I saw and I'm like -- when I say I saw, how can I see an electronic signal, all I can see is a display on a monitor. … And I was told that the display that I was watching was a visualisation of data moving in and out of GSOC. …and data was coming into GSOC via the same device. I saw that and it went on for an extended period."*

He said that intelligence agencies have "sleeper devices" which enable data to be stored over extended periods onto a hard drive and then downloaded over the router of the hotspot.

The Closing Report

9.31. Following the operation conducted on 19th November 2013 the investigation officers briefed Commissioner Fitzgerald and the Chairperson on 25th November 2013 to the effect that there had been no "positive result". The Chairperson then made a note in his personal log: "*This investigation is now closed. I need to think about reporting. This will be difficult, we have found nothing."* A report upon the investigation was drafted in accordance with Section 101 of the Act. This task was undertaken mainly by Officer C as Officer A was about to depart on extended leave to carry out work for an international agency abroad. Following receipt of the third Verrimus Report of Mr [redacted] on 16th December 2013, Officer C finalised that report, signed it and presented it to Officer B. This is the "Closing Report" on the Public Interest Investigation commenced on 8th October 2013.

9.32. The Closing Report set out in detail the steps that had been taken during the course of the investigation and outlined the contents of the three reports received from Verrimus.

9.33. In relation to the threat posed by the unusual behaviour of Device 4B, the author of the report concluded that the investigation had provided no technical explanation as to how that device had been able to connect with the Bitbuzz network. He described how, using software supplied by Verrimus and following their instructions, Device 4B had been monitored during office hours between 2nd and 11th November. The monitoring disclosed no discernable pattern of behaviour. The device showed an 'historic connection' to the AMX system but no connection to Bitbuzz historic or otherwise and took varying amounts of time between 10 minutes and 5 hours to establish a live connection. He considered that the behaviour of the device was more likely to be due to some unknown technical anomaly rather than its having been used for unauthorised technical or electronic surveillance.

9.34. The Closing Report also described the conducting of the "alert test" on the Polycom unit and the subsequent requisitioning of information from Eircom which provided no record of the 'ring-back call' on the morning of 27th September. GSOC's IT Department had also extracted a list of all calls made to or from the extension number of the Polycom unit between 29th August 2012 and 27th September 2013. This recorded no indication of the ring-back call on the morning of 27th September either but did show a record of the call that Officer A had made from that unit to the extension of the Chairperson's desk phone.

9.35. In relation to the detection of the UK 3G code on the iPhone, the Closing Report stated that Verrimus had indicated that this detection was *"good evidence of a localised intelligence-gathering or interception device."*

9.36. The conclusion to the Closing Report stated that the investigation in question had been initiated *"After information known only to senior management of the*

*Ombudsman Commission was repeated by a third party to the Ombudsman Commission Chairperson."*

9.37. In evidence to this Inquiry Officer C acknowledged that this statement was due to a misunderstanding on his part. He had not been involved in any of these matters prior to being briefed by Officer A for the purpose of the investigation on 8th October 2013. Prior to that briefing he had been unaware that the security sweep of 23rd-27th September 2013 had taken place.

The Verrimus Expert

9.38. Evidence on behalf of Verrimus Ltd was given by Mr [redacted], [redacted] at the company. Mr [redacted] confirmed the description given by the GSOC officers as to how his firm came to be contacted and engaged for the purpose of carrying out the surveys in September 2013. He was the author of the TSCM Report and the CC1/002 Report. He was present on all three visits to the GSOC offices in September-November 2013. On each visit he was accompanied by one or more Verrimus colleagues and on 9th November 2013 by Mr [redacted]. He explained to the Inquiry the scope and purpose of the 12 surveys or tests carried out during the first visit and described and explained the equipment used for those purposes in general terms. Mr [redacted] explained the reference made in the TSCM Survey Report to *"a perceived threat and quantifiable evidence of a verbal indicator of eavesdropping"* as deriving from the background information which had been given to him by the investigating officer as to the lead up to commissioning the surveillance sweep. He had been told that a phrase discussed in one of the areas to be covered by the sweep had been repeated by someone outside GSOC and this had raised concerns because the phrase was very specific and had been mentioned in a report.

9.39. In advance of an interview conducted on 16th April 2014 Arthur Cox submitted a detailed statement which he had made out accompanied by a file containing some 49 supporting exhibits. The statement greatly expanded upon and explained the information and assessments contained in the TSCM and CCI-002 Reports and gave a step-by-step account of the tests conducted and the measures taken during the three visits to GSOC. The statement listed and described the various pieces of equipment used in the tests and surveys. This was later supplemented by his further statements mentioned in paragraphs 9.60 and 10.15 below.

First Visit - Device 4B

9.40. As already described above, the first detected threat was that of the unusual behaviour of Device 4B. He explained that a wireless network access point is the means of entry to the network rather like a door to a building and should be protected by an appropriate level of security like a door lock. The particular WEP security on the GSOC AMX network was regarded as wholly insecure and was easily hacked even by someone without special training. The significance of the weakness in the security of the wireless access points in question was that an eavesdropper could gain access to the microphone-enabled units connected on the network in the Boardroom and the Media Room and use them to listen to conversations in those areas.

9.41. Mr [redacted] s analysis also indicated to him that the Research Electronics International (REI) white noise generation system ANG-2200 installed in the Boardroom would not work against eavesdropping audio attacks in those areas. An attacker would be able to eavesdrop on conversations in the Boardroom via access to the conference microphones over the insecure wireless network and thereby have unrestricted audio feed from the room unhindered by the noise generator system.

The Polycom Unit

9.42. Mr [redacted] explained in greater detail the tests that had been carried out on the Polycom unit which had led to the conclusion that the telephone line to the conference extension equipment had been intercepted or "tapped" by some eavesdropper. An "analogue audio test" was carried out using a "TALAN" device which was placed "in line" that is, between the telephone device and the telephone exchange. Measurements can then be taken of the telephone and the telephone line in normal function and the line can then be tested by applying room audio. There should be no room audio when the telephone is not active. The telephone is then put into "off hook" mode, the handset is lifted thus opening the line. Each wire pair is then tested again for the presence of room audio. There should be no room audio present on certain wires only. This is the "alerting test" already mentioned above which can alert any eavesdropper to the fact that the telephone device is being tested for technical surveillance attacks. On this occasion loud music was used as room audio for the test. The test carried out showed no abnormality so the telephone device was put back in its normal state. Within approximately three seconds of cancelling the test and putting the phone back in its normal state, the Polycom unit rang showing "unknown number."

9.43. Mr [redacted] testified that he had personally carried out this same test on thousands of telephones and had never previously encountered this occurrence. All of the settings on the phone test device were checked to ensure that it had not generated this reaction. The test was then carried out twice more to ensure that there was no system fault but the same ring-back reaction did not occur again. He subsequently contacted the manufacturer of the test device and was assured that it was not possible that the test could have caused the ring-back reaction given the settings that were being used and that no bias generator was involved.

9.44. Officer A queried whether it could be a coincidental wrong number that had caused the phone to ring. They then tried making a call to the GSOC switchboard and the call was directed immediately to the GSOC out-of-office message indicating that it was impossible for the call back to have come through the switchboard. It could only, accordingly, have come by way of a direct dial to the extension number of the Polycom unit. It was on that basis that Mr [redacted] suggested that the chance of someone randomly dialling that particular wrong number at that time of night from an "unknown number" was so small as to be "virtually zero." Mr [redacted] said that he had also ruled out the possibility that the ring-back reaction was attributable to the PBX reacting to his test device by testing other telephones in the building on the night in question without obtaining the reaction.

9.45. Accordingly, having ruled out various other possibilities, Mr [redacted] gave it as his firm opinion that the only explanation for the ring-back occurrence was that some inexperienced operator charged with monitoring the telephone line, having noticed

that the line was activated in the early hours of the morning and hearing the loud music, unthinkingly suspected a connection fault and made the mistake of ringing the monitored device to test the intercept system. He therefore listed the occurrence as a threat *"as it is an anomaly that has no benign explanation in scientific testing."* He considered that his assessment was subsequently confirmed by the information received from Eircom that no call had been placed to the Polycom unit extension number at the time. In other words, the interception which caused the Polycom unit to ring must have occurred at a point between the Eircom exchange and the GSOC PBX. He insisted that the TALAN device test carried out in the way he described cannot cause the telephone device to ring in this way. He pointed out that if a telephone handset is picked up and one sings down the line and then puts the handset back on the hook, the phone will not then ring you back. A telephone system requires voltage in order to make it ring. Playing music or noise down the line does not create voltage.

Second Visit

9.46. Mr [redacted] then described in greater detail the visit on 19th-20th October 2013. By process of elimination Device 4B was located and identified. It was found not to be usable for its intended purpose as its touch screen was broken but the device was still powered on. On 19th October monitoring of Device 4B noted that it appeared no longer to be probing for the Bitbuzz network as it had been on 26th September.

9.47. The further scans were resumed on the morning of Sunday 20th October 2013. On this occasion Device 4B was observed to be connecting directly to the Bitbuzz network in the adjacent store/coffee shop. As the device had a built-in microphone it was considered that there was a present threat that the microphone could be used by an attacker to eavesdrop on conversations. Mr [redacted] asked his Verrimus colleague to go down to the shop in question where the colleague observed a man wearing a baseball cap using a tablet device. Device 4B was communicating with the Bitbuzz network and "data packets" were observed to be exchanged. This was monitored throughout the day. Mr [redacted]'s colleague's phone was connected to the Bitbuzz network in order to demonstrate the effect communication on the network has on the increase in the rate of packet transfer. It was observed that the packet rate increase on the 4B/Bitbuzz was far greater than on the exchange between the colleague's phone and Bitbuzz, thus suggesting that the communication of data was greater in volume on the Device 4B/Bitbuzz transfer. Because Device 4B device's only sensor was a microphone, it was apparent to him that, on the balance of probability, the data packets being transmitted consisted of room audio content only.

9.48. Mr [redacted] also described two further incidents that occurred on this occasion. First, while he and his colleague were working on the communications console in the cupboard in the Boardroom they noticed one or two *"same individuals"* who appeared to *"be making inordinate attempts to watch what we were doing from the street."* Secondly his colleague, while in the coffee shop, and believing that an audio attack was functioning, noted an unknown male enter carrying a nylon sports bag which appeared to contain what he described as *"a large box-shaped item that looked very heavy as the individual was carrying the item on his back and the object inside was distorting the shape of the bag it was so heavy."* The colleague, a former chief inspector and police detective with extensive experience in intelligence-gathering techniques, saw this as an indication of localised technical intelligence-gathering. He

turned on his iPhone's scanning function to scan for all carriers in the area. This showed the normal Irish networks but additionally showed the country code and network code five digit identifier of another network which was subsequently identified as one allocated to a UK network of a group also operating in the State. This test was subsequently repeated at various times with two other phones both in the coffee shop and the GSOC offices but the unusual network code was not again detected.

9.49. Mr [redacted] described the particular network code in question as an "obscure code" and he ruled out the possibility that this was attributable to the operation in the area of a UK femtocell. He had tested one such device and found that it broadcast the legitimate UK code and not the obscure code that had been detected. Furthermore, he had confirmed that the UK service provider in question had deliberately configured their femtocell devices to ensure that they would not be able to operate outside the United Kingdom.

9.50. He also expressed the view that it was highly improbable that anyone would use a UK femtocell merely to avoid roaming charges given that free communication was available over applications such as Skype.

9.51. Mr [redacted] then described an incident that occurred following the conclusion of the visit to GSOC on this occasion. At Dublin Airport, having checked in and passed through security and while waiting to board at the departure lounge, he and his colleague were sitting in a corner seat with their backs to a blank wall when they were approached by an unknown individual who stood directly in front of them and took out a camera from his shoulder bag. They turned away to avoid being photographed but the individual waited and when they turned back he photographed them. Mr [redacted] described this as a "trade craft procedure" known as being "burned" which is a strategy used by the "opposition" to let them know that they are aware of their presence and that, in other words, "their cover has been blown."

9.52. In his first written statement Mr [redacted] summarised his conclusions on the surveys and tests of 19th-20th October in these terms:

- *"GSOC did not maintain information relating to what devices are authorised or unauthorised on the wireless conferencing system, as they did not have or maintain wireless network records.*
- *GOS did not have the skill set or capability to test the wireless conferencing network.*
- *Client 4B is a conferencing console which is part of GSOC's wireless conferencing network. It is not able to carry out its main function but is still active and situated in a secure meeting room.*
- *Client 4B is microphone enabled and was evidenced connected outside of its own network, to a public internet access point. Contrary to what the manufacturer describes as its normal function, which* (sic) *is something they say should not be possible without manipulation.*
- *Client 4B whilst illicitly connected to a public internet access point is passing data packets (communicating).*
- *There were suspected physical surveillance personnel active in the areas as detected by [*a GSOC officer*],* [redacted] *(*his colleague*) and myself.*

- *There was a "fake" UK mobile phone network detected and evidenced by* [redacted] *which was very short range and only lasted for a short time, which is symptomatic of an IMSI Catcher surveillance device.*
- [redacted] *and myself were "Burned" at the airport."*

9.53. In his evidence at interview Mr [redacted] was firm in his conviction that GSOC offices and personnel had been under active covert surveillance by means of the three threats that had been detected. He was convinced that the Device 4B had been tampered with and "manipulated" for the purpose of enabling it to connect to the Bitbuzz network. He was fully satisfied that there was no explanation for the ring-back occurrence on the Polycom unit other than the telephone line to that extension having been intercepted or tapped. He was equally satisfied that the only explanation for the appearance of the UK 3G code was the presence in the vicinity of an IMSI catcher.

Third Visit

9.54. Mr [redacted] then described the work done on his third visit on 19th November for the special operation which had been set up by the Investigating Officers. He described this as a "sting operation to draw out the user" which he had suggested. The objective was to monitor the false information meeting set up by the officers for any unauthorised surveillance activity and if any such activity was detected to identify and locate the devices being used. The work also involved examining and disassembling the AMX panel consoles to see if there were any signs of their being used by way of attack. He was accompanied on this visit by two other Verrimus operatives and Mr [redacted]

9.55. As already indicated by other witnesses, this special operation did not result in the detection of any surveillance activities. Mr [redacted] did however comment upon the results of Mr [redacted]'s forensic examination of Device 4B. He pointed out that as he had himself seen the device "actually connect" to Bitbuzz, the device should in his view have had a record of that connection in its systems files. He concluded that Device 4B had been cleaned or wiped of that information and expressed the opinion that this could well have been done remotely without the attacker having needed to physically access Device 4B. In his opinion Device 4B showed signs of having been tampered with. Its components had been changed and its systems files had been tampered with. In his statement he said, *"A tamper proof seal was broken and other visual signs of human interference were present. Finger smudges around internal screw holes being most of note."* Moreover, it indicated that it had been cleaned or wiped since it had been last detected as connecting to Bitbuzz on 20th October 2013.

9.56. When asked if the connection he observed meant that Device 4B was actually logging into the Internet through the Bitbuzz hotspot Mr [redacted] replied *"That's impossible to tell from our survey. Our survey identifies that it's connected and communicating whilst connected to that network. That would require investigation at a level which we can't carry out".*

9.57. Mr [redacted] summarised his opinions by stating that, on the balance of probability:

- The AMX conferencing system had been compromised and could be used to eavesdrop on conversations in one or both areas of the Boardroom and the Media Room;
- Devices 4B (and also possibly Device BC) had been "cleaned" or "wiped" prior to the forensic examination in November 2013;
- There was physical surveillance being conducted in the area of the GSOC premises on 20th October 2013; and
- There was no benign explanation for the ring-back reaction of the Polycom unit on 27th September 2013.

9.58. In conclusion, Mr [redacted] emphasised that his work was concerned only with detecting vulnerabilities and areas of potential attacks upon the GSOC communications' systems. He did not have and was not invited to express any opinion as to who might be responsible for any possible eavesdropping or illicit surveillance. Insofar as the description of "intelligence-service level" surveillance is attributable to the reports furnished by his company, that is explanatory only of the level at which such equipment may be lawfully used. He recognised that in the dark world of surveillance and counter-surveillance highly sophisticated and up-to-date equipment may well be available illegitimately to a wide range of parties for wholly unlawful use.

9.59. Following consideration of the information and assessment provided by Mr [redacted] in his statement and interview, I requested Arthur Cox to ask him for clarification of a number of points and to consider some additional possible explanations of the anomalies. I also asked that he review the service records of device 4B in order to consider whether they might provide an explanation for the "tampering" he had described. Furthermore, Mr McEnroy SC insisted that in the interests of fair procedures, GSOC was entitled to require that Verrimus as its 'servant or agent' was placed in a position to comment upon and respond to any information or advice furnished to the Inquiry which bore upon the findings or assessments of the threats as detected and explained by that firm.

9.60. Having been accommodated by me in that regard, on 12th May 2014, Arthur Cox submitted a supplemental statement by Mr [redacted] The main points made in this statement can be summarised as follows:

- The Verrimus task was confined to conducting a counter-surveillance sweep to identify any possible areas of potential threat or security vulnerability. It reported the detected anomalies to GSOC but had no mandate or authority to investigate them.

- All the measures and procedures referred to in its reports and evidence *"are based in espionage and counter-espionage domains and are not readily evidenced or explained through open source knowledge or information. Nor are they properly quantifiable by experts outside those domains. Any qualification of evidence, facts or opinions can only safely be made by an operator with equal or greater knowledge and experience in technical surveillance counter-measures."*

- With regard to the possible explanation for the detection of the UK 3G code described in paragraph 9.70 below (the communication with the UK test bed) he asserted that this did not explain the whole results of the original findings. *"If this*

*was the reason for the detection, then it would have been detected on multiple occasions in multiple locations."* If it was in fact the test signal that had been detected, it must have been fortuitous in that it was picked up at the precise moment the test was carried out and was then turned off and was not subsequently detected at other times when tested throughout the day. This he said was a most unlikely explanation.

- With regard to the connection of Device 4B to the internet he maintained that any device can be programmed to automatically connect to hotspots and pre-authenticated automatically. Authentication needs to happen only once then a device can automatically connect on future occasions. With regard to the apparent absence of any retained record of Device 4B having authenticated to the Bitbuzz network, he maintained that this was not definitive as the absence of information on the device could be due to its having been wiped. He maintained that the control test already detailed proved that the device was acting as a fully authenticated device and successfully passing audio and data over the connection and had been evidenced with a far higher data packet rate at multiple times during the day of the monitoring.

- In relation to the service/maintenance documentation he made the following points:

    - No hardware fixes were detailed as having been undertaken for Device 4B when listed as faulty on 25th May 2009 leading to the reasonable assumption that maintenance is not the reason for the signs of physical tampering;
    - Firmware up-grades on the AMX system were noted on 28th February 2011 and 5th September 2012 while the [redacted] Report had noted an anomaly in the last access dates on Devices 4B and BC showing 1st January 1970, 6th December 2006 and 10th January 2031. [redacted] was of the opinion that system files should therefore have shown last firmware up-dates as on the actual dates it was evidenced as being carried out. This strongly supported the suggestion that data on both devices had been wiped at some point. Evidence of both devices being wiped suggests that both could have been used to eavesdrop in their respective areas.

- He also commented in relation to the Rits firm that *"whilst obviously very respected in the IT security domain, [they] were wholly the wrong type of company to review a TSCM-based report. Their report could only have been peer reviewed by an independent and expert TSCM operator."*

- In relation to the testing of the line to the Polycom unit, he stated that the test equipment and procedures used are the same for both analogue and digital telephones and the equipment in question is the only TSCM equipment currently available with the requisite technical capacity. He maintains that an eavesdropper could easily have heard the audio test as music even if it had been converted to a digital signal. All they would require is a device with the correct digital codec[3] and these are commercially available.

[3] See Appendix II

9.61. Mr [redacted]'s evidence was further added to in a third statement submitted by Arthur Cox on 29th May 2014. (See paragraph 10.15 below)

Postscript

9.62. Mr [redacted] also mentioned in evidence that he had availed of his four days in Dublin between 23rd-27th September 2013 to visit some other prospective customers with a view to interesting them in training courses and in the equipment his company could provide. These included a visit to the Garda Síochána Security Division where he demonstrated a number of up-to-date counter-surveillance devices. He then described a number of phone calls he received shortly after the announcement of the establishment of this Inquiry. Counsel for GSOC submitted that the transcripts of these calls were proper to be drawn to the attention of the Inquiry as GSOC was concerned they represented an attempt to influence the evidence to be given to and the conduct of this Inquiry. The evidence in question is dealt with in Appendix III below. This evidence was added to by Mr [redacted] in the supplemental statement referred to above. He said that he had since again been approached by the individual in question at an exhibition where he once more sought to convey to Mr [redacted] the views of the Garda Síochána on the involvement of Verrimus in Ireland. The individual claimed to have been specifically asked by his Garda Síochána contacts what Mr [redacted] was doing and that this was the reason why he had telephoned Mr [redacted]

The Bitbuzz Hotspot

9.63. Enquiries were made with the provider of the Wi-Fi service in the nearby shop. Bitbuzz Ltd is an Irish company which specialises in the provision of public access to the internet at locations usually referred to as "Wi-Fi hotspots." Its customers are typically retail outlets and public buildings such as hotels, restaurants, coffee shops. It provides the service according to a variety of business models. In the context of the present Inquiry the relevant model is that in which Bitbuzz installs and manages a Wi-Fi access point to the internet in a retail premises such as a coffee shop. This enables the proprietor of the outlet to offer free Wi-Fi connection to the internet to its customers. The proprietor typically pays Bitbuzz for the provision, management and servicing of the installation and the promotion of the service. Because such an outlet will wish to encourage a constant turnover of its own customers, the free access will normally be limited to a period of twenty minutes or thereabouts.

9.64. In order to make use of this service the retail customer with a smart phone or laptop must register in some form with Bitbuzz. Registration on the Bitbuzz network requires the user to provide his or her name, e-mail address and a contact phone number. Registration can also be procured through a Facebook or a Twitter account and in that form a unique account identifier is provided to Bitbuzz but not the name, e-mail address and phone number. Certain mobile phone service providers also purchase wholesale access to the Bitbuzz network and subscribers to those networks can also access and authenticate to the Bitbuzz hotspot through the mobile phone account. The relevant identification particulars of a registered user are retained by Bitbuzz as required by the Communications (Retention of Data) Act 2011. The stored details include both the MAC and ID address but for fully authenticated customers only.

9.65. When a Wi-Fi device such as a smart phone or laptop first seeks to connect to a Bitbuzz hotspot, the hotspot will automatically assign an IP address to the device in question. This step is described as the device "associating" to the access point of the Bitbuzz network i.e. the hotspot. At this point the device has no access to the internet and is firewalled from it and from the Bitbuzz database. To take the further step of gaining access to the internet through the hotspot, the device must "authenticate" to the Bitbuzz network and, in effect, become registered as a Bitbuzz customer providing the identification particulars mentioned above. Once authenticated and registered as a Bitbuzz customer the MAC address of the device will automatically be recognised and will authenticate on any other hotspot of the Bitbuzz network without the necessity for a new authentication step.

9.66. Bitbuzz allocates a limited number of IP addresses for use at each hotspot depending upon the size of the outlet and traffic likely to be attracted. If a device associates to the hotspot and receives an IP address but does not proceed to authenticate to the customer database, the IP address in question may be reused and assigned to a different device. When a device probes for an adjacent internet access point and seeks to associate with an available public Wi-Fi hotspot, in order to be allocated an IP address for the purpose, traffic occurs consisting of three or four "internet packets" exchanged between the device and the network.

9.67. The Wi-Fi access point cannot connect itself to a device. The initiative to make the connection must come from the device. Furthermore, no one gaining access to the internet elsewhere could connect with and communicate to a device through the Bitbuzz hotspot unless the target device has come on line to the hotspot and been authenticated. Moreover it is not normally possible for an internet user elsewhere to make an in-bound connection to an authenticated user in a Bitbuzz hotspot. The firewall normally allows only connections by authenticated users from inside the hotspot to the outside, for example to a web page. A user outside wanting to communicate with a device inside the hotspot could do so only if the device on the inside had set up an outbound "tunnel" connection to a pre-arranged server and allowed the remote user to connect via that connection. This would have to be set up on the device in the hotspot and would require particular software and configuration.

9.68. It is, however, in theory possible that two devices associated to but not authenticated to the same hotspot simultaneously could effect communications between them. This would require both devices to be simultaneously present within range of the Wi-Fi signal.

Information on the UK 3G Code

9.69. Enquiries were also made of the Irish mobile phone company whose sister company's code in the UK was detected on the iPhone scan. The information supplied confirmed that two of the alternative explanations for the detection of the UK code were untenable. The company confirmed that all of the equipment used in its Irish network had been purchased direct, as new, from its manufacturers and as already configured for use in the Irish network. No possibility therefore arose of a UK base station being imported and re-used or reconfigured for the Irish network. Secondly, it was not possible that the detected code could have been generated by a UK femtocell being manipulated and used in this country in order to avoid roaming charges. The

particular code in question would not be generated by a UK femtocell issued by the UK company.

9.70. The company did, however, offer a further explanation as to why the country/ network code in question might have been detected on that occasion. In common with other mobile phone service providers in this jurisdiction, the Irish company had been allocated the new 4G/LTE spectrum in 2012. In September-October 2013 it was in the process of rolling out and testing the equipment for that new service in a number of locations in Dublin including one close to Upper Abbey Street. As the core network for the 4G service here was not yet in place, these tests involved connecting to the group's test bed which is located in the United Kingdom. The particular detected 5 digit country/network code is one that is allocated exclusively to that test bed and would have been generated only by communications with the test bed. Furthermore, only the company's own engineers held SIM cards configured for communicating with the UK test bed. The company considered it likely that it is these tests which may have caused the detection of the code. The tests in question started on 5th September 2013 and ceased on 31st October 2013.

Audio-Visual System – Service/Maintenance Records:

9.71. At my request GSOC extracted all of the job sheets, service records and maintenance documentation and invoices for the AMX audio/visual system from its original installation in 2007 until 2013. This indicated that apart from annual routine servicing, the equipment including the AMX touch panel remote controls had been reported faulty on a number of occasions and had been repaired, rebooted or reconfigured. For example on 25th/26th May 2009 the AMX touch panel in the Boardroom was found to be faulty, was removed from the offices overnight, repaired and re-programmed and reinstalled. The job description on the engineer's work sheet notes: *"reconfigure existing touch panel."* A job card for a repair visit in March 2011 recorded that the work done included rebooting the AMX controllers in both rooms. As already mentioned, I interviewed the principal of the firm that had carried out the annual service and some repairs to the equipment since 2011. He explained that their work in servicing, repairing and any re-booting or reconfiguring the AMX system devices had never involved opening up Device 4B(or Device BC). The configuring, reprogramming or rebooting of the device is effected through the external contacts on the panel without any need to access the internal components. He and his operatives would therefore have been unaware of any removal and replacement of any of the manufacturer's original components in Device 4B. For any repair that involved access to internal components, the touch panel would have been sent to the manufacturer but this had never arisen since their contract engagement commenced in 2011.

9.72. He also confirmed that, as shown in the documents for the dates in question, Device 4B had been found to be faulty in April 2012. It was powering up but no signal from it was being picked by the receiver in the communications console. The firm provided quotations for a number of options to remedy the situation including repairing the existing system or installing a new replacement.

9.73. None of the options was taken up and on a call-out visit in on 19th February 2013 the service engineer's report on the two touch panels of the audio/visual equipment records, *"AV system controller failures in Boardroom and Media Room."*. On the

subsequent annual service visit on 4th March 2013 the record shows, *"Boardroom unit faulty, Media Room ok."* In his first statement Mr [redacted] in describing Device 4B had said: "*Its only intelligence sensor is a built-in microphone."* This interviewee confirmed the point made by Officer A (paragraph 9.29 above) that the device did not have a built-in microphone. Its function was to communicate wireless instructions for the various sources of input (lap-top, projector, DVD player etc.) in the conference audio/visual system.

Report under Section 103 of the Act

9.74. The information and results required by Section 103(1) of the Act was eventually furnished to the Minister by the Chairperson of GSOC in a written report on 13th February 2014. The report follows broadly the terms of the Closing Report (see paragraph 9.31-9.36 above). It summarises the course of the investigation of the suspected surveillance from the commencement of the security sweep until the Closing Report in December 2013. It describes the steps taken during that period by the investigating officers and the Verrimus experts. It then summarises the conclusions reached by GSOC on the P.I. investigation. In respect of Device 4B the conclusion given was as follows:

> *"7.1 Test conducted by the security specialists and designated officers have consistently shown that Device 4B, a component part of the AMX audio/visual system, had been establishing a connection to the Bitbuzz network. This system has been located at business premises near the Ombudsman Commission offices since August 2013. The investigation has not been able to provide a technical explanation as to how Device 4B was apparently able to connect to the Bitbuzz network.*
> *7.2 As the AMX audio/visual system in the GSOC offices used a WEP Vulnerable Encryption….Device 4B had the potential to be used to gain control of the devices and data on the AMX audio/visual system.*
> *7.3 The investigation has established that the AMX audio/visual system was wired according to the manufacturer's specification. There was no evidence of a connection between this equipment and the Ombudsman Commission's network/servers.*
> *7.4 Given that the Bitbuzz network was only installed in the nearby business premises two months previously and with the limited data potential available from the AMX audio/visual system, the designated officer took a view that it is likely that Device 4B's behaviour was due to some unknown technical anomaly rather than it having been used for any unauthorised technical or electronic surveillance."*

9.75. The conclusions in respect of the anomaly on the Polycom unit was as follows:

> *"9.1 Telecoms enquiries have revealed no trace of the call received by the conference call unit at approximately 0.1-0.2 hours on 27th September 2013. However, two witnesses verified that during the test on 27th September 2013, the conference call unit received a call of around three rings in duration. As the organisation's switchboard was on out-of-hours service, this call must have been made direct to the conference call unit."*

9.76. The report then describes the detection of the UK 3G network code on 20th October 2013 and fives the conclusion:

> *"10.3 Subsequent enquiries indicated that the code was the identifier for a 3G telephone service provider in the UK. The security specialists attributed its detection, on Sunday 20th October 2013 to an interception device in the area. They described this as being good evidence of localised intelligence-gathering.*

*10.4 Absent any further clarification, the Commission could not simply proceed on the basis that these issues were purely innocent or coincidental. Accordingly the Commission conducted a specific operational test on 19th November 2013; this was coordinated by the security specialists and involved a GSOC investigation team. It also involved the three Commissioners to test these issues. This operational test yielded no results and added no clarity to the threats identified above."*

9.77. The overall conclusion was then given in paragraph 11 of the report as follows:

*"The GSOC investigation did not find any definitive evidence that GSOC was under technical or electronic surveillance. It did, however, uncover a number of technical and electronic anomalies that cannot be explained."*

Interview of Commission Members

9.78. As already indicated, on 19th May 2014 I met with the three members of the Commission both to clarify some matters that had arisen during the course of the Inquiry and to afford them an opportunity of commenting upon the conclusions and recommendations which I had it in mind to make in this report. Shortly before the meeting, the Commissioners submitted a signed statement which summarised the position of the Commission in respect of the statutory investigation which had been carried out into the detected security threats.

9.79. They emphasised that having decided to carry out a security sweep, they had retained Verrimus Ltd on the basis of recommendations received from the other comparable statutory authorities and the professional competence, standards and methodology of the technical exercise which had been undertaken by Verrimus had been confirmed to them by an independent specialist technical review obtained from Shearwater TSCM Ltd.

9.80. They stated that the reports furnished by Verrimus identified specific threats to the security of the GSOC officers and the fact of the existence of those threats is not in dispute. Those threats needed to be investigated to discover whether their existence and level of possible compromise could be established or disproven. This meant that GSOC needed to establish their provenance, capability and history. The possibility that Garda misconduct might be identified meant that it was important to ensure any relevant evidence was gathered in a statutory framework. These enquiries were urgent and required the use of police powers. The statutory investigation was therefore properly authorised and the personnel concerned were acting bona fide in discharge of their statutory duties as investigators.

9.81. The Commissioners expressed the view that the suggestions made in the Rits Report seeking to undermine the Verrimus Reports are not credible. Furthermore, the series of third party efforts made to influence the evidence to be given to the Inquiry by Verrimus are unexplained and of concern. They expressed the view that *"There is no credible expert opinion that disputes the existence of the threats identified"* by Verrimus.

9.82. The statement points out that the Commission had not said that it had identified a particular individual or entity who sought to gain access to sensitive information in the Commission's possession. *"This does not, however, detract from the fact that a set of circumstances existed which required investigation."*

9.83. In relation to the exercise of the power in S.102 (4) the Commissioners maintained:

> *"The language employed in S.102 (4) provides a very broad discretionary power to commence an investigation. There is no requirement in S.102 (4) to establish precedent facts or proof of facts to an evidential standard. That approach is inconsistent with an investigative function and is more appropriate to an adjudicative task. A fair approach to the identified matters of concern required the exercise of the statutory powers of S.102 (4). The law has long recognised a series of incremental evidential standards that it applies depending on the legal context, the statutory purpose and the stage of the investigative process. At one end of the evidential spectrum is suspicion and the other proof beyond reasonable doubt. There is no reason in law why a different approach should be adopted to statutory investigations by the Commission. The concerns identified properly justified the exercise of the statutory power in S.102 (4) to commence an investigation. An investigation was impossible without the use of statutory police powers. Those concerns were based on objective facts. Neither the benefit of the hindsight nor a different view of the same facts disturbs the honesty or legitimacy of the assessment of those facts made at the time and the decision to commence the investigation into those concerns."*

## 10. Review and Assessment:

10.1. Paragraph 3 of the Terms of Reference requires that the evidence and information available to the Inquiry in relation to the facts and events covered by paragraph 1 of those terms should be reviewed and assessed. It is appropriate to do so by reference first to the three particular 'threats' or anomalies which had been detected and formed the subject matter of the investigation carried out by GSOC under Section 102(4) as described above.

Device 4B

10.2. This device was found, when identified by the Verrimus scan to have been performing abnormally in that it appeared to be connecting (or at least attempting to connect) with an internet access point outside the Wi-Fi network of the audio/visual conference system in the GSOC offices. Verrimus classified it as a "threat" to the security of that system because it gave rise to the possibility that an external third party could gain access to the device and receive at least audio data from it. Initially it was not known whether the Wi-Fi network in question had any connection to other databases or servers. Even when this possibility was eliminated the abnormal behaviour of the device still constituted a serious threat to the security of communications within the room and on the conference system. It is important to note that Verrimus was asked to conduct its survey in order to identify all possible vulnerabilities to the security of communications within GSOC in the areas in question. It was not concerned with determining whether actual breaches had in fact occurred although it appears to have

proceeded on the assumption that one had because of the briefing that it had been given. This abnormal behaviour of Device 4B was classified as a "threat" because it was a device located in an area required to be secure which was performing in a way that ought not to have been possible if it had not been tampered with and its normal configuration to the AMX system altered.

10.3. In the light of the information in the retained data supplied by Bitbuzz to GSOC and of the explanations as to the manner in which access to the internet through the hotspot is obtained or permitted, there does not appear to be any concrete proof that Device 4B at any stage subsequent to the installation of the hotspot in question in August 2013 actually authenticated to and registered on the Bitbuzz network so as to open up an internet connection between Device 4B and any third party internet user. It appears likely that the traffic observed when Device 4B was monitored as connecting or seeking to connect to the Bitbuzz network consisted of the network packets that are exchanged when such a Wi-Fi device probes for the network in order to associate to it. Even if the traffic was considered to include data packets of audio data from the room, such data could not have been accessed through or communicated over the internet in the absence of evidence that Device 4B ever successfully authenticated to the Bitbuzz network. Had it ever done so either during the observation of 20th October 2013 or on any earlier occasion since August 2013, its identifying particulars would have been registered and retained in Bitbuzz customer database. The retained records provided to GSOC by Bitbuzz for the period 19th to 21st October disclosed no such evidence.

10.4. This assessment has been, of course, rejected by Mr [redacted] as described above both in his evidence and the first of his supplementary statements. Although as cited in paragraph 9.56 above, Mr [redacted] had said in evidence that it was impossible to tell from his survey whether Device 4B while being monitored was actually authenticating to the Bitbuzz network so as to be accessible to the internet, he maintained that the control test described in his first witness statement established that the device must have successfully authenticated and logged into the network. This was based on the comparison that had been made between the packets exchanged by Device 4B and the corresponding traffic observed when his colleague's iPhone fully authenticated to the Bitbuzz hotspot and transmitted data over the internet. In his supplementary statement he said that the control test proved that:

> "*4B was acting in the exact same manner as a proven fully authenticated device, a device which was successfully passing audio and data over that connection, in fact 4B was evidenced with a far higher data packet rate at multiple times during the that day. An event which it had not carried out at all on the previous whole day of testing, and thereby strongly suggesting that this was not a random occurrence."*

10.5. There appear to be a number of reasons why this is not fully convincing. First, it does not appear to be in doubt that if the device had fully authenticated to the Bitbuzz network on 20th October 2013 or at any prior date, its MAC address would have been retained in the Bitbuzz network database as required by law. As already indicated, Mr [redacted] considers that the absence of such a record is *"not definitive"* because *"that lack of information on the device could only have been due to it being wiped."* But it is not the absence of the connection record in the memory file of Device 4B that is

significant but the absence of the MAC address retained in the Bitbuzz database. It does not appear to be suggested or plausible that the supposed attacker had gone to the length of hacking into the database in question in order to wipe from it any record of that MAC address.

10.6. Secondly, the comparison in the apparent volumes of data packet transfer rates between Device 4B and the mobile phone merits more detailed consideration. The data which is being communicated between the device and the hotspot router is broken down and transmitted in blocks which may vary in size depending upon the type of network being used between 64 bytes and 2,312 bytes. The actual data content of any packet/block may be less than its full capacity. Accordingly, the numerical count of data packets observed may not represent a valid quantification of the actual content being communicated. In his original witness statement Mr [redacted] supports his explanations in this regard by reference to a number of screen shots taken from the scanning equipment which was used to monitor the data communications in question. (Exhibits 36, 37 and 42). In these screen shots it is possible to identify in the top portion of the screen the various Wi-Fi networks available in the area including the GSOC AMX network, the Bitbuzz network and a number of broadband routers in the vicinity. In the lower part of the screen shots it is then possible to identify by reference to the MAC addresses of the Bitbuzz hotspot and Device 4B the packets being transmitted by Device 4B to Bitbuzz on the one hand and from the colleague's phone to Bitbuzz on the other. Thus, in Exhibit 36, Device 4B is shown as associated to the Bitbuzz IP address and having exchanged 121 data packets. The colleague's phone although shown as *"not associated"* has 350 packets. Similarly in Exhibit 37 where both devices have associated to the Bitbuzz MAC address, Device 4B has 388 data packets and the phone 187.

10.7. Thus, the numerical count of data packets observed as being exchanged between Device 4B and the Bitbuzz hotspot does not, as such, constitute proof that Device 4B has fully authenticated to the Bitbuzz network. In this regard it must be borne in mind that Device 4B is a somewhat rudimentary device based on technology which is now obsolete and was never intended to do anything more than communicate input instructions within the audio/visual conference system, Device 4B could have continued repeatedly to probe for connection thus generating what appears to be a high number of data packets without necessarily transferring any corresponding high volume of actual data. It is also possible that the discrepancies in the volumes of traffic apparently observed from Device 4B and the phone are explained by the substantial differences in their respective hardware and software. To validate the comparison suggested by Mr [redacted] as a basis for demonstrating that device 4B had fully authenticated to the Bitbuzz network, it would have been necessary to capture and analyse the data packets in question using equipment and software that is available for the purpose. This was not done as it was not part of the Verrimus remit which was concerned primarily with locating areas of vulnerability so that they could be eliminated.

10.8. To fully eliminate any possibility that Device 4B had ever actually authenticated to that network it would be necessary to extract and examine the record of all retained data for the hotspot from the date of its installation in August 2013 in order to

determine whether the MAC address of Device 4B had fully authenticated and registered.

10.9. Even if it is highly probable that Device 4B never actually authenticated to the Bitbuzz network, there remains the question as to how it came to be behaving in this anomalous way? Mr [redacted] gave as his conclusion that the device had been tampered with and therefore manipulated "*for the purpose of enabling it to connect to the Bitbuzz network."* In his principal statement he said, after having contacted the help desk of the manufacturer of device 4B in the USA about the anomaly, *"This is not a random event. Client 4B has been manipulated on purpose to connect to Bitbuzz."* When asked about the tampering at interview and whether he considered it had been done for the purpose of getting it to connect to Bitbuzz he said: "*I have no idea. All I can say is it was tampered with."* The use of the word "manipulated" might be thought pejorative and to beg the question in this context but it is nevertheless clear that some reconfiguration or altered configuration of the device must have occurred in order for it to function in a way it was not designed to do as a piece of equipment in such a conference system.

10.10. The effect of the [redacted] report of the forensic examination of Device 4B's components together with Mr [redacted]'s assessment of the significance of the threat posed by its anomalous behaviour as referred to above at paragraphs 9.40 and 10.9 is to imply a causal link between the discovery of the replaced components as tampering and manipulation on the one hand and the apparent ability of the device to connect to the hotspot on the other. In the light of the fact that the configuration of the touch panel is effected externally through the contact points, it is clear that the 'tampering' by replacing the manufacturer's original components has no necessary relation to the anomalous behaviour of the connection to the Bitbuzz network. This is the point made by Officer A as indicated at paragraph 9.28 above.

10.11. Furthermore, in the briefing note provided to the Minister by GSOC on 10th February 2014 and in the appearance before the PSOP Committee on 12th February 2014, the concern expressed at the anomalous behaviour of Device 4B was explained in part by the knowledge that it was password protected and that *"absent this password, the device should not have been able to connect to that external Wi-Fi- network."* It was said that no-one in GSOC knew the password.

10.12. It transpires however that all AMX touch panels of this model are supplied with the same default password '1988' which is published in the "Quick Start Guide" for them on the manufacturer's website. The possibility cannot be excluded therefore that a service engineer finding Device 4B faulty endeavoured to diagnose the fault by seeing if it would connect to an available open Wi-Fi network in the vicinity.

10.13. It is also possible of course that someone else familiar with those instructions and with the freedom of access to the offices within GSOC carried out the configuration in question and presumably did so at some point after the installation of the hotspot in the coffee shop in August 2013. This is the view of Mr [redacted] as mentioned below.

10.14. In the light of this information I requested that an engineer from the service company test Device 4B to see if the original manufacturer's default password had ever been changed. On the instruction of Arthur Cox on behalf of GSOC the firm carried out a

technical review of the AMX components of the conference audio/visual installation and with the letter of 29 May 2014 the legal representative furnished me with a report which confirmed that "[all] passwords for access to the AMX components are factory default and have not been changed." The report also points out that the components of the AMX system are connected through an access point which generates a SSID which can be picked up in the adjacent coffee shop. Attempts to access this SSID via a laptop or phone resulted in the access point logging the attempted connection and then dropping it.

10.15. In view of the confirmation that Device 4B was not 'microphone-enabled' and the fact that its password was unchanged, I invited Mr [redacted] and GSOC to submit any further comments they might wish to have considered. On 29th May 2014 Arthur Cox submitted a second supplementary statement from Mr [redacted] with the report from the maintenance engineer mentioned in paragraph 10.14.

10.16. Mr [redacted] acknowledged that it had been assumed that Device 4B had a built-in microphone because it had a microphone hole, *"...an airspace specifically made by a manufacturer to allow vibrations to pass through the case to a microphone"*. He pointed out, however, the reference in his first statement to, *"The use [by an attacker] of the built-in microphone to eavesdrop"* was a description of the system and not just of the handset as a component part. The vulnerability still exists throughout the network. He pointed out that:

> *"... should the system contain any other intelligence sensors, or control any other intelligence sensors, microphones, cameras or communication devices, the level of 'threat' does not diminish. It is merely a requirement, once a vulnerability (Threat) to the system is established, to investigate it fully to establish if an attack is present or if there is historic sign of attack or if there is a benign explanation for the vulnerability. Something which was not our remit, nor could we give a more accurate opinion as we were not given Network Diagrams, as they did not exist."*

10.17. In relation to the information that the default password of the device had not been changed he commented that this meant that:

> *"... anyone could reprogram the units to control any part of the system. The fact that the controller's handsets were broken means no physical inspection would be able to tell this, leaving any reprogramming attack physically undetectable. On compromise any software alterations could be easily wiped leaving no evidence, merely historic sign of being wiped."*

10.18. He also commented upon the attempts made (see paragraph 10.14 above) to access the SSID of the device:

> *"10. ... This is an irrelevant test in the circumstance as if there were an attack gateway it would no doubt have been 'removed' given the now pubic nature of this enquiry etc. In any case, such attacks are usually MAC address specific to allow only the attackers device to effect the attack, making it difficult to accidently find.*

11. *Any investigation to 'find' an attack at this stage is in my experience not likely to find evidence. Any technical surveillance operation has measures to remove evidence if compromised. Any attack that may have been in place, would have been thoroughly cleaned once it was suspected it was compromised, let alone in the public eye."*

Detection of the Fake UK 3G Network

10.19. As explained above, the five digit code attributed to a UK mobile phone network provider was detected on the iPhone screen of the Verrimus operative as one of the mobile phone networks apparently available in the locality of the GSOC office. The Verrimus expert considered that this *"was symptomatic"* of an intelligence-gathering operation in the vicinity and when evaluated in conjunction with the other observations that were made on the occasion in the area, led to the conclusion that the explanation lay in the presence of an IMSI catcher.

10.20. As explained in paragraph 9.69 above, alternative explanations suggested in the Rits Report as to how the code might have been transmitted can be ruled out. However, the fact that the particular five digit code is attributed to and generated only by a test bed belonging to the UK operation of the network in question makes it highly likely that the detection was caused by the testing of a new 4G installation by that network which is confirmed as having been taking place over the period of weeks during which the detection was made. Notwithstanding the questions raised by Mr [redacted] in his supplementary statement above, it is highly likely, accordingly, that the detection of the code that was observed did not originate in an IMSI catcher but with the tests being conducted at the time by the network in question. The information from the mobile phone company is that the particular 5 digit MCC/MNC code is allocated exclusively to the UK test bed of the sister company. What benefit could a covert eavesdropper expect to achieve by using it as a false base station as opposed to using the code allocated to the actual UK 3G network used by its UK customers?

The Polycom Unit

10.21. This anomaly was classified as a security threat by Verrimus because of the unexplained ring-back which occurred upon it following the conducting of the "alert test," in the early morning of 27th September 2013. Its other tests did not apparently provide any evidence of the line having been compromised and the result could not be replicated when the alert test was repeated. As already described, this occurrence was classified by Verrimus as a security threat because the ring-back appeared to have no scientific explanation. The Verrimus expert was strongly of the view that the only available explanation was that of a somewhat careless monitoring agent unthinkingly intervening to phone the extension. This attribution of the occurrence to human error would appear, on the face of it, to be somewhat at variance with the premise that GSOC was being subjected to a sophisticated surveillance attack which was characterised as at intelligence service level.

10.22. More importantly however, that explanation appears to be based upon the proposition that the eavesdropper monitoring the tap on the line will hear the alert as music as would be the case when a simple tap is placed on a copper wire of an analogue phone line. It is at least questionable whether this would be possible when it is the case that

the test alert signal on the analogue line of the Polycom unit must have been converted to a digital communication by the PBX analogue card for onward transmission over this digital line (with all other communication traffic from GSOC) through the Government's secure central network. This suggestion is firmly rejected by Mr [redacted] in his supplementary statement. All the eavesdropper would require he says, is a device with the correct digital codec[4] which is commercially available. It remains the case however that this 'ring-back' occurrence has not been explained and further extensive tests in conjunction with the device's manufacturer would probably be required to advance the matter further.

Physical Surveillance

10.23. There remains the description given by the officers and by Mr [redacted] of the suspected physical surveillance of the GSOC building on the occasion of the second visit on 19th-20th October 2013 – the white van in the street; the two men observed by Officer A; the man with the heavy sports bag in the coffee shop and the photographer at the airport.

10.24. It is notable that when these incidents were being evaluated by the investigating officers they had been aware of Mr [redacted]'s visit to the Garda Security Division in September. At the time however the possible significance of that fact does not appear to have been appreciated. On the face of it, there would hardly be surprising if the Security Branch knowing that UK counter-surveillance experts were in Dublin with very sophisticated equipment, had an interest in the identities of their other potential clients. In his evidence, with the benefit of hindsight, Officer B expressed the view that it was probably the Verrimus personnel that were under surveillance and not the GSOC offices. He said:

> *"It's the cynical me who has been around the block on these things. I believe that our countersurveillance operation had been detected and that the IMSE Catcher was there to detect the UK operators who were in our building at the time with a view to determining what they were at, the extent of what they were doing and what they might actually know. And it wasn't so much GSOC that was being targeted so much as Verrimus."*

In the interview of 19the May 2014 the Commissioners gave me to understand that they had been informed by the Garda Commissioner that no operation in the vicinity of the GSOC offices had been in place on 20th October 2013.

General Observations

10.25. It is appropriate to add one further general observation in respect of the TSCM Survey Report having regard to the importance which was attached to it as the basis for the commencement of the P.I. investigation. In view of the circumstances in which it was commissioned, of its purpose and of the client for which it was addressed, it is open to the criticism that, in the absence of further explanation in non-technical language, the manner in which its findings were expressed carried the risk of conveying to a non-

[4] See Appendix II

expert reader an exaggerated understanding of the significance of its findings. While understandably highly technical, the use of terminology in the sense understood within the counter-surveillance craft such as "Red Flag Warning", "multiple threat detected"; "guaranteed threat"; "very highly vulnerable", equivalent to "almost certain" and "hostile attack" was liable to be construed as giving a heightened assessment of the anomalies detected in the absence of an explanation as to the relevance of the limitations which the report itself identifies. These included the absence of network diagrams and other basic information; the insufficiency of the time to locate Device 4B and the lack of information as to whether there existed any actual connection between the audio/visual system and the data storage servers, computers and other equipment or facilities in the GSOC offices.

10.26. Furthermore, the presentation of the findings is not always easy to follow. For example, one of the listed "Red Flag Warnings" is of a threat detected in the conduct of the "Full physical domain search." That term is not used elsewhere in the TSCM Survey Report and it was not until Mr [redacted] explained the report in evidence that it became apparent that the threat in question was that of the inadequacy of the white noise system ANG-2200 which had been identified under the "Full Wi-Fi threat detection survey" as one of the "multiple threats detected".

10.27. A similar observation can be made in relation to the CCI-002 Report. The characterisation of the assumed threat as *"up to intelligence service attack level"* might be regarded as an inappropriate assumption as the basis for commencing the work of the second visit when, for example, Device 4B had not yet been located or examined. Similarly, the description of the detection of the UK 3G code on 20th October 2013 as *"good evidence of a localised intelligence-gathering or interception device"* and *"symptomatic of something in the nature of a dedicated 3G IMSI grabber or interceptor"* could be read as a definitive finding in the absence of any mention of other possible explanations even for the purpose of explaining why they should be excluded.

10.28. It is also somewhat surprising that when Device 4B was judged to be connecting with and transferring data to the Bitbuzz network, consideration was not given to the question as to how the device could actually be set up and configured especially when the basic instructions for the purpose were available on the manufacturer's website.

10.29. It might also be considered surprising having regard to the importance placed upon the vulnerability of the audio/visual system to eavesdropping through access to its microphones that when Device 4B was dismantled for forensic examination, the absence of the microphone it had been assumed to contain was not drawn to the attention of the investigating officers.

## 11. Conclusions

11.1. In the light of the above review and assessment of the evidence and the totality of information made available to the Inquiry and, subject to the reservation indicated in paragraph 1.5 above, it appears possible to provide the following conclusions by way of opinion:

1) Although, as the members of the Commission themselves concluded and stated to the Minister and the PSOP Committee, it is impossible on the basis of the technical opinions and available information, categorically to rule out all possibility of covert surveillance in the three threats identified by Verrimus, it is clear that the evidence does not support the proposition that actual surveillance of the kind asserted in the Sunday Times article took place and much less that it was carried out by members of the Garda Síochána.

2) So far as the threat detected in the abnormal functioning of Device 4B is concerned and notwithstanding the technical opinion given by Verrimus, it seems highly improbable that the haphazard performance of such a remote control device constituted the planned means of covert eavesdropping on GSOC in a sophisticated surveillance exercise by any agency equipped with a capability of "intelligence service level." Furthermore, having regard to the technical limitations of gaining access to the device over the internet by an external third party as described in paragraph 9.67 above, it seems implausible that such a mechanism would have been used and that steps had been taken to "wipe" all traces of the connection and to circumvent the statutory data retention records of the database of the network in question. Furthermore, the possibly sinister characterisation attributed to its abnormal behaviour appears now to warrant reconsideration in view of the fact that: a) it was not microphone enabled as had been assumed; and b) its original default password was publicly available and had not been changed.

3) Having regard to the explanation given by the mobile phone network in relation to the testing of the 4G/LTE equipment at the time, it is clearly more probable that the iPhone scan detection of the country/network code was not caused by the presence in the vicinity of the offices of an IMSI catcher, notwithstanding the points to the contrary made by Verrimus as indicated in paragraph 9.61 above.

4) The fact that the communication with the test bed of the mobile phone company in the UK may provide an explanation for the detection of the UK code in question does not, of course, rule out the possibility that there was also an IMSI catcher being deployed in the area at the time. But if that were so, why would the third party engaged in covert surveillance make use of the "obscure" test bed code to create a fake base station rather than the code allocated to the network used by the subscribers intended to be targeted?

5) The 'ring-back' reaction to the alert test of the Polycom unit remains unexplained as a technical or scientific anomaly. As indicated, there appear to be some technical factors which cast doubt upon the explanation that there had been mistaken human intervention in the monitoring of a tap upon the phone line outside the GSOC offices although Mr [redacted] has maintained that the use of the correct digital codec would have enabled the eavesdropper to have heard the digital signal as music. Whatever the explanation may be, there is no evidence that the ring-back reaction was necessarily attributable to an offence or misbehaviour on the part of a member of the Garda Síochána.

6) In view of the additional information that has come to light in this Inquiry, it is possible in retrospect to see that an investigation in the public interest under

Section 102(4) of the Act on 8th October 2013 was not at that date immediately necessary and was possibly a premature recourse to the power contained in that provision. At that date the only matters available to the Commission by way of indication of the existence of the statutory conditions of that provision were the detection of the abnormal behaviour of Device 4B and the unexplained nocturnal ring-back on the Polycom unit. The specific device generating the apparent connection to the Wi-Fi hotspot had not then been identified or located. In effect, what had been detected were two technical anomalies and possible malfunctions in particular pieces of equipment. As such, the information available did not indicate that an offence had been committed or that disciplinary misbehaviour had occurred. Nor did it indicate that if the anomalies were to be attributable to third party surveillance or intervention on those GSOC devices, that a member of the Garda Síochána might be responsible.

7) At that date, 8th October 2013, further tests and enquiries, including most of those subsequently conducted by Verrimus Ltd on 19th-20th October might have been undertaken to eliminate malfunction as explanations of the anomalies before recourse to s.102(4) was had. Some of the non-statutory enquiries made in the course of this Inquiry demonstrate that information available without the exercise of statutory investigation powers could have allayed some of the alarm caused by the manner in which the 'Red Flag Warnings' of the TSCM Report were expressed.

8) Because it was considered that an offence or misbehaviour by a member of the force could possibly be the cause or origin of one or more of the two TSCM survey threats, it was thought necessary to conduct the further investigation within a statutory framework so that the powers under S. 98 of the Act would be available and any evidence would be admissible in any resulting proceedings. In the event, the only such powers used were those for the obtaining of records from Bitbuzz and Eircom and then only after suspicions were heightened by the third detection on 20th October 2013. Use of the powers of arrest had been contemplated for the 'special operation' of 19th November 2013 and in the event were not needed.

9) Having commenced, conducted and then closed an investigation in the public interest pursuant to section 102(4) of the Act, there was an obligation upon the Commission to furnish information in relation to its results to both the Minister and the Commissioner. This was the mandatory obligation that arises under Section 103(1) (b) of the Act and not the discretion which the Commission has under Section 80(5) of the Act to make a special report to the Minister drawing attention to matters of gravity or exceptional circumstances that have come to its notice. Although the Commission appears to have been conscious of this obligation to report, it was not until after the publication of the Sunday Times article that the non-compliance was remedied on 13th February 2014. On that date a written report was furnished to the Minister. The written report was not given to the Garda Commission but the Chairperson informed this Inquiry that the Garda Commissioner had been given a verbal report to the same effect. The Commission had always proceeded on the basis that the requirements of S. 103(1) could be met either verbally or in writing.

10) It is difficult to avoid the impression that the concerns generated by the Red Flag Warnings in the first TSCM Report and the interpretations placed upon those and on the subsequent detections and events, were heavily influenced by the atmosphere of frustration and tension that had arisen in relations between GSOC personnel and the senior ranks of the Garda Síochána thus leading to the raising of suspicions which might not otherwise have been acted upon.

11) It is also clear, however, that the investigating officers and the members of the Commission acted in good faith in taking the steps in question once presented with the TSCM Report. Indeed it is understandable that, presented with the existence of two apparently serious threats to their security, their primary concern was to move quickly to take the steps necessary to investigate and, if necessary, counter those threats. They were possibly unduly alarmed by the language used and perfunctory exposé of the findings presented in that report. It is unfortunate that further elucidation and advice from Verrimus or a second opinion was not sought before the P.I. investigation was commenced. That said and as indicated above, Mr [redacted] has remained adamant that his survey results prove that some form of covert surveillance had taken place.

12) It should be made clear nevertheless that this retrospective view of the reality of the detected threats neither intends nor implies any criticism of Officer B in performing his duty by deciding to direct the P.I. investigation nor of the Commissioners in approving that decision. They were presented unexpectedly with an apparent result they did not anticipate from the security sweep which understandably caused great concern, even alarm, having regard to the terms in which the findings were expressed. They had carefully chosen and then relied upon expert advices from a reliably recommended specialist firm.

13) So far as concerns the suspicions of physical surveillance – the white van and the two men who turned away; the men observing the Verrimus operatives from the street; the man with the heavy sports bag in the coffee shop and the photographer at the airport – having regard to the demonstration visit made by Verrimus to Garda Síochána Security Branch in September, it seems highly likely that such surveillance (if that is what it was) was directed at the activities of Verrimus operatives rather than at GSOC personnel. This impression would appear to be supported by the contents of the phone calls subsequently received by Mr [redacted] as described in Appendix III.

14) There is no evidence which links any such physical surveillance to any one or to all of the three 'threats' thought to have been detected.

15) It will be apparent from much of the material covered in this Report and from the divergent opinions of those with technical expertise, that in the somewhat febrile world of covert surveillance and counter-surveillance techniques, it is ultimately extremely difficult to determine with complete certainty whether unexplained anomalies of the kinds identified in this instance were or were not attributable to unlawful intrusion. The range of technologies and devices available for the conduct of remotely sourced and untraceable eavesdropping or interception of different forms of communication, is such that it is difficult categorically to

exclude the possibility that some form of illicit eavesdropping may have taken place.

16) It is no doubt possible that further tests and investigations might be conducted with a view to finding explanations for the anomalous behaviour of Device 4B and the Polycom unit. These would obviously involve consulting the manufacturers of the two items. In the case of Device 4B it would require tracing its pre-2011 maintenance and repair history with a view to establishing how, when and by whom the original components had been replaced and whether that had any causal link to its abnormal behaviour in September 2013. As mentioned in paragraph 10.8 it would also be possible to ascertain from the Bitbuzz data base whether the MAC address had ever been registered prior to 20th October 2013. Tests might also be conducted to establish whether the fear expressed by Officer A at paragraph 9.29 above had any foundation namely, that the connection (if any) made to the hotspot by Device 4B was capable of being exploited to hack into the entire conference system.

17) Having regard to the absence of evidence that the anomalies in question were in fact exploited for the purpose of illicit surveillance and to the fact that their threat potential has since been eliminated it may be questionable whether such further investigations would be justified.

18) So far as concerns the incidents of suspected physical surveillance on 20th October 2013 any further investigation to ascertain whether those suspicions were well-founded could only be carried out in an appropriate statutory framework as it would require the availability of powers to compel the provision of information and access to documentary and other records.

## 12. The Sunday Times Article

12.1. It is clear of course that the information "revealed" in the Sunday Times article of 9th February 2014 is evidence of a serious breach of security of GSOC's confidential information because, although seriously inaccurate, it appears to have its source in information known only to those who were privy to the conduct and outcome of the P.I. Investigation. That being so, the investigation of that breach is unrelated to the supposed threats which were the subject of the P.I. Investigation and therefore outside the remit of the present Terms of Reference. I have been informed that the breach in question is the subject of an internal enquiry by GSOC.

12.2. Having regard to the character of that breach, its investigation is not in any event suitable for an *ad hoc* non-statutory inquiry of the present kind with no competence to compel the provision of information and no authority to determine issues of fact or resolve disputes as to truth and credibility. It will be noted, however, that the article contains misinformation in relation to the investigation and its outcome. GSOC's "Wi-Fi network" was not compromised to "steal e-mails, data and confidential reports". Insofar as the sweep examined a "Wi-Fi network" it was confined to the wireless devices of the audio-visual equipment and was unconnected to any data storage. There was no "second Wi-Fi system" which had been created using an "IP

address in Britain". No "Government owned technology" had in fact been used to "hack into e-mails".

12.3. It is a matter for GSOC's internal enquiry or for any future statutory investigation that may be considered necessary or desirable to determine whether there was any link between the obvious leak of the information on which the Sunday Times article was based and the possibility inferred to in paragraph 10.13 above that someone with access to the Media Room and familiarity with the password was responsible for the configuration of Device 4B.

## 13. Recommendations

13.1. Paragraph 4 of the Terms of Reference invites the making of recommendations regarding measures to improve existing security arrangements and addressing any risks to data and communications in GSOC.

13.2. The security sweep carried out by Verrimus identified a series of vulnerabilities in the GSOC offices, equipment and technologies designed to ensure confidentiality. While the actual anomalies thus identified may not be shown to have in fact been exploited to carry out covert surveillance, it is obvious that the vulnerabilities such as the WEP encryption being obsolete, the inadequacy of the REI perimeter and the lack of security in the conferencing Wi-Fi equipment should be addressed and rectified. I have had described to me the steps taken, or in the course of being taken, by GSOC since September 2013 to address those faults and deficiencies. It would obviously defeat the effectiveness of those measures to describe them in this report. On the basis of technical advice given to the Inquiry in that regard, however, I am satisfied that the steps taken are adequate to rectify the defects and vulnerabilities and sufficient to enhance the security of the relevant areas and the equipment used in them. The AMX touch panels are no longer used and while conference phone call equipment is still necessary, measures have been adopted to ensure that it is not used for sensitive or confidential communications. Coincidentally and not as a result of the findings of the security sweep, the entire telephone system has been replaced. The Commissioners explained to me that GSOC has been operating with a reduced staffing complement as a result of budget restrictions and the moratorium on recruitment and this has an impact upon the resources available to implement optimum security measures. They consider that GSOC is vulnerable in the absence of the proposed disaster recovery site at its Longford office for which approval from the Department of Public Expenditure and Justice and Equality has not been forthcoming.

13.3. The only other recommendation that falls to be made under this heading, accordingly, is that GSOC should more frequently carry out a thorough and suitable counter-surveillance examination of its offices, communication and IT equipment and data storage facilities to ensure that its protection remains adequate and that the risk of new surveillance techniques being deployed against the Commission or its personnel is reduced as much as possible. Similarly, it is obviously necessary that staff are trained and updated regularly in the procedures and strategies needed to mimimise the risk of their being personally compromised in the use of communications equipment.

13.4. The invitation in paragraph 5 of the Terms of Reference to make more general recommendations may perhaps have been superseded since the Inquiry was established by the announcement that legislation will be introduced to establish a new police authority. This would suggest that pending legislation will define the function of such an authority and necessarily revise the roles and relationships of GSOC, the Garda Commissioner and the Minister in the light of the introduction of that authority.

13.5. In that event it might be considered desirable to take account of some issues that have been raised by the events described and the information made available to this Inquiry. I would recommend, for example, that consideration should be given to clarifying the precise scope of the competence to be accorded to GSOC to conduct investigations of its own initiative under section 102(4). Should that competence be

more explicitly confined to the investigation of matters which are attributable only to the possible commission of an offence or misbehaviour by one or more identified (or potentially identifiable) members of the Garda Síochána? Or, is it considered desirable as a matter of legislative policy that the power be exercisable in circumstances where the offence or misbehaviour may be possibly attributable exclusively to third parties who are not members of the force?

13.6. I acknowledge that when this possible lack of precision in the subsection was raised by me with the Commissioners, both in the interview of 19th May and subsequently in the letter of 29th May 2014 from Arthur Cox, strong objection was made to any recommendation for amendment mainly on the ground that it would be *"likely to be suggestive of some form of criticism of a professional officer of GSOC"*. It was complained in that regard by Arthur Cox that *"we still do not know the information that has grounded this provisional recommendation"*.

13.7. It is important to point out that this recommendation is not made by way of criticism of any GSOC officer as suggested. It is based entirely on my doubts as to the correct interpretation of the subsection as it stands in the light of the general issue raised by the peculiar circumstances of this case where the information in consideration on 8th October 2013 can be seen on the one hand, as merely indicative of two possible technical malfunctions in two pieces of GSOC equipment unrelated to any offence or misbehaviour by anyone; or on the other, as possibly attributable to some illicit intrusion although not necessarily by any member of the Garda Síochána. The existing wording is undoubtedly open also to the interpretation hitherto given to it by GSOC. I merely recommend that in any revision of the Act of 2005 in this regard the question as to which interpretation reflects the intention of the legislature might be addressed.

13.8. Finally, if there is to be new legislation redefining the roles of and relationships between the Commissioner, the Minister and GSOC in the context of introducing the new police authority, it may be desirable to consider simplifying the somewhat complex provisions governing the making, admissibility and investigation of complaints as currently contained in Part 4 of the Act in the light of the experience of their operation since 2007. The Commissioners rightly place an important value on the comparatively open nature of the existing complaints regime. They understand that the rationale behind the distinctions made, for example between complaints made within or outside a garda station and different ranks of members, lies in the need to avoid misunderstandings or complications in distinguishing between an actual complaint and the content of an accusation or altercation between a garda and a member of the public on the street. Nevertheless, if new legislation is proposed which will revise or expand the investigative remit of GSOC it may be desirable to consider whether in the light of experience some of the distinctions and conditions embodied in Part 4 continue to be necessary.

# APPENDIX I

## Chronology of Facts and Events

| | |
|---|---|
| **2012** | During 2012 the newly appointed members of the Commission met on a number of occasions with the Garda Commissioner (and on occasion with his deputies) and discussed GSOC's concerns about the delays being encountered in important current investigations in obtaining timely responses to requests for information and documents and the need for adherence to the existing protocols. |
| 15th May | The Chairperson met with the Secretary General of the Department and raised with him the problem of procuring timely access to requested information and documents from the force in the particular context of two investigations then current. |
| 30th June | The GSOC Annual Report for 2011 was published which referred to these delays in the provision of information. |
| 20th September | The Chairperson again met with the Commissioner and raised the question of delays in the provision of information to investigations. The Commissioner on the other hand raised concerns about the extent to which confidential information in relation to some current investigations was appearing in the press. |
| 16th November | The Commissioner phoned a member of the Commission raising concerns in relation to media coverage of one investigation. |
| 18th November | An article appeared in the "Sunday Times" on the investigation. Further articles appeared in that newspaper on 9th and 16th December 2012. |
| 13th December | A file on the investigation was sent to the DPP. |
| 17th December | The Garda Commissioner again contacted the Commission with concerns about the information appearing in the press. |
| **2013** | |
| 4th February | A further discussion about the delays took place between the Chairperson at a meeting with the Commissioner and his deputies. |
| 23rd April | The DPP directed that no prosecution be brought in the investigation. |
| 29th April | Commissioners Fitzgerald and Foley met the Minister and indicated that in reports to be presented the Commission would make public criticism of the Garda Síochána. |
| 2nd/7th May | A report on the investigation was sent to the Minister and to the Commissioner in accordance with s.103 of the Act. |
| 9th May | A Special Report under section 80(5) of the Act was submitted to Minister who laid it before the Oireachtas. |

| | |
|---|---|
| 23rd May | The GSOC Annual Report for 2012 (together with a press release) was published containing criticism of the failures of the Garda Síochána to abide by the existing protocols. |
| 4th June | The Chairperson discussed with the Director of Administration the possibility of conducting a security sweep of the offices and enquiries were made as to the availability of the Irish security firm which had conducted one in 2007. It was found to be no longer available. |
| 9th June | A further article appeared in the Sunday Times about one of the investigations. |
| 3rd July | The GSOC Commissioners appeared before Joint Oireachtas Committee on Public Service Oversight and Petitions (PSOP) to discuss the 2012 Annual Report and the Special Report under s.80 of the Act. (See 9 May above.) |
| 16th July | Designated officers discussed the Chairperson's meeting with Garda Commissioner on 24th July. |
| 23rd July | Meeting of Chairperson with the Minister, the Secretary General and Garda Commissioner which discussed the s. 80(5) report, the negotiations on protocols and the issue of timeliness of information. |
| 24th July | Chairperson met Garda Commissioner to discuss further the above topics and the investigation. |
| 24th July | Chairperson briefed designated officers on meetings of 23rd & 24th July. |
| 24th-25th July | Enquiries are made with UK equivalent authority the IPCC on suitable counter-surveillance expert firm. |
| 12th August | First contact by the Senior Investigating Officer (SIO) with Verrimus. |
| 21st August | The Designated Officers agreed to instruct SIO to engage and instruct Verrimus to undertake sweep. |
| 23rd August | The SIO briefed Verrimus. |
| 26th August | Acting Director of Investigations instructed SIO to have Verrimus add two additional rooms to the sweep. A new quotation is sought and furnished by the firm. |
| 28th August | The Commission gives approval to proceed. |
| 17th September | Verrimus proposal for sweep is presented to the SIO, discussed with the Acting Director of Investigations and approved. The Chairperson is briefed. |
| 23rd September | New Protocols are signed by the Chairperson and the Garda Commissioner. |

| | |
|---|---|
| 23rd-27th September | Security sweep conducted by Verrimus at GSOC offices over 28 hours. Threats 1 and 2 are detected. |
| 27th September | On-line test of Polycom unit carried out at 1.40 am |
| 7th October | First Verrimus Report, the TSCM Survey Report, was received by the designated officers and assessed. |
| 8th October | The Acting Director of Investigations informed the Chairperson of the detected threats. It is agreed that full provenance of the threats must be established quickly. A Public Interest Investigation is initiated by the Acting Director of Investigations under s. 102(4) of the Act with the agreement of the Chairperson. The Chairperson later briefs Commissioner Foley on the steps that have been taken. |
| 9th October | Verrimus is re-engaged to conduct further investigation into the threats. |
| 19th-20th October | Revisit and tests by Verrimus: detection of the third threat, the code of a UK 3G network base station and suspected "IMSI Catcher" |
| 21st October | Commissioner Fitzgerald returns from leave and is briefed on the developments and steps taken. |
| 23rd October | Authorisations are given to obtain retained records of communications and phone calls from Bitbuzz and Eircom. |
| 24th October | Meeting with Bitbuzz representative |
| 25th October | Data supplied by Bitbuzz |
| 29th October | Second Verrimus Report CC1/002 furnished. |
| 2nd-11th November | GSOC investigation officers monitor activity of Device 4B |
| 11th November | A new Director of Investigations takes up duties. |
| 19th November | A special "operational test" involving the Verrimus operatives and the Designated Officers of the investigation team is conducted at the GSOC offices. Tests by KJB Forensics. |
| 25th November | The Chairperson and Commissioner Fitzgerald are briefed by the investigation team on the fact that the tests on 19th November had produced no positive result. The Chairperson noted that the investigation was closed and that nothing had been found. |
| 17th December | Closing Report of GSOC drafted by Officer C under s.101 of the Act was furnished to the Deputy Director of Investigations. |
| 17th December | S. 102(4) Investigation closed. |
| 17th-19th | The S.101 Report was finalised by Officer B to the Director of Investigations and in turn to the Chairperson. The Director of |

| | |
|---|---|
| December | Administration then placed it in a safe. |

**2014**

| | |
|---|---|
| 4th February | The Director of Administration brought the S.101 Report to the Chairperson's attention and later returned it to the safe. |
| 9th February | The Sunday Times article was published. |
| 10th February | Briefing note provided to Minister by GSOC |
| 12th February | Appearance of Commission at PSOP Committee |
| 13th February | S. 103 Report on the PI. Investigation submitted to the Minister. |
| 19th February | Establishment of this Inquiry |

# APPENDIX II

## Glossary of Terms

### Ambient Listening

This term describes a technical stratagem whereby an eavesdropper or attacker can both intercept calls made to and from a telephone (whether mobile or land line) and use the receiver as a listening device through which conversations on and in the vicinity of the telephone receiver can be overheard and recorded without the knowledge of the owner of the phone and without leaving any trace.

Once an eavesdropper knows the number of the target phone (and other details?) and has the necessary equipment, it is possible remotely to activate the microphone in the instrument and leave it turned on. It can be left turned on indefinitely in the case of a landline receiver and in the case of a mobile phone, so long as its battery retains power.

One of the effects of an ambient listening attack on a mobile phone is that it can cause an unusually rapid depletion in its battery.

### IMSI Catcher/Grabber

This term describes a piece of equipment which enables an eavesdropper to intercept and track mobile phones by mimicking the function of a mobile phone network tower or mast so as, in effect, to intervene between the user of the mobile phone and the network on which the user is a subscriber. In essence, it is a false mobile phone base station. The initials IMSI stand for International Mobile Subscriber Identity. When a mobile phone user makes a call the handset will seek to connect to the nearest base station of the subscriber's network. The handset is required to authenticate to that network but it is not necessary that the network authenticate to the handset. The IMSI catcher by mimicking the function of a base station, causes every mobile phone on the simulated network to log into it and forces phones to transmit the international mobile subscriber identity of the handset. Because the encryption of phone data traffic is chosen by the base station, the IMSI catcher can force the connected mobile phone to use no call encryption thereby making data easy to intercept and convert to audio.

Although an IMSI catcher operates as a fake base transceiver station, the equipment involves no structural equivalent to the typical roof top mast of a network. As the technology has developed, the equipment has become smaller and mobile. Versions of the device are now becoming available which are of size capable of being worn on the body and concealed underneath an overcoat.

Furthermore, as a simple search of the internet will demonstrate, IMSI catchers are readily available on the open market so that their use is not confined to official intelligence services or police forces. Units are available from companies such as Gamma International and Forensic Telecommunications Services. They can be bought for less than €500.

The significance of the interception threat posed by an IMSI catcher will be apparent from the fact that some units are capable of operating simultaneously as fake base stations for a number of networks and can harvest over 1,000 IMSI's within 60 seconds. It follows that the detection of a false country code amongst a number of network codes does not mean that it is the false foreign network alone that was the target of the IMSI catcher. If the IMSI catcher is

capable of operating multiple fake base stations at the same time, it could be targeting the legitimate local networks as well.

**MAC Address**

MAC stands for 'Media Access Control': the MAC address is a unique 12 digit identifier assigned by a manufacturer to a wireless device (referred to as a 'client device') capable of communicating with a network including a computer network

**Femtocell**

A small cellular base station supplied to residential or small business customers of mobile networks to enable the subscriber to connect to the mobile phone network via broadband in areas where the signal may be weak.

**MCC/MNC**

Stands for mobile country code/mobile network code and is the identifying number assigned to each mobile network service provider. It usually comprises 5 digits of which the first three identify the country of the service provider and the remaining two digits are the code allocated in that country to the particular network. The MCC for Ireland is 272 and for the UK is 235.

**Codec**

This term derives from "coder-decoder" and describes a computer program which can decode a digital data signal or stream for playback.

**SSID**

Stands for Service Set Identifier and is the name given to a wireless network. On any Wireless Local Area Network (WLAN) the wireless devices intended to be used must have the same SSID if they are to be able to communicate with one another.

# APPENDIX III

## Post Inquiry Phone Calls to Verrimus Limited

As mentioned at paragraph 9.61 above, subsequent to the establishment of this Inquiry, Mr [redacted] of Verrimus Limited described in his evidence to the Inquiry that he had received a number of phone calls from an individual whom he knew and who appeared to be concerned to discuss with him the evidence which Mr [redacted] would give to the Inquiry.

The individual in question was a businessman who is engaged in Ireland in supplying and in acting as manufacturers' agent for a range of equipment of the kind used in surveillance and counter-surveillance work. Mr [redacted] had first encountered him in 2013 at a trade exhibition in London. The individual had been interested in establishing a business relationship with Verrimus Limited.

Counsel for GSOC felt it proper that the content of these conversations should be drawn to the attention of the Inquiry because GSOC had concerns that this approach represented an attempt to influence the evidence to be provided to the Inquiry.

The conversations had taken place on 19th and 25th February 2014. The conversations are lengthy and quite oblique for the most part but one theme appears to have been a desire on the part of the individual to convey concerns that had been expressed to him by contacts in both the Garda Síochána and Irish Army Security Services. A flavour of the principal threads in the conversation can be gleaned from the following extracts of what was said by the caller to Mr [redacted]:

25th February 2014 – first call:

CALLER *"Well, you know, one of the things that may come out of this, [redacted] when you speak with the Judge ... Is to impress upon him that that particular aspect of things that actually that you would like the Gardaí would actually get a copy of everything, right. ... And, you know, try to impress upon him that, you know, that it's in everyone's interest that all of this should be out in the open and that everyone could talk about it, because what it actually means to them, [redacted] right, is that if he would be monitored doing what you were doing, by somebody, right then that is a criminal matter and that is something that needs to be investigated."*

CALLER *"Right. And they should be investigated by the powers that be and in this case that means the Gardaí need to know exactly what it is that you actually discovered. So that would be one of the primary things I believe that should come out of all of this."*

25th February 2014 – second call:

*"MR [redacted]: And, you know, the problem that we have when we go to the see the judge is that the judge isn't a technical man so his… Because the likes of his understanding is probably as little as Minister Shatter or Rits.*

*CALLER: Well, you know, there is work going on behind the scenes there to put in a man in there who may understand the whole significance of it. Right. And I know that the boys in green are trying to get a man who is, let me say.*
*MR [redacted]: Is in to advise?*
*CALLER: Someone who would know what he was on about, he would know exactly who I would be talking about right.*
*MR [redacted]: Will I recognise him when I walk in?*
*CALLER: No, no, you would never have met this individual.*
*MR [redacted]: All right. Good.*
*CALLER: You would never had met this individual. This is an individual who would have been in a similar appointment.*
*MR [redacted]: All right, okay.*
*CALLER: In other words, retired.*
*MR [redacted] All right, I understand no problem. Well, he has been briefed about me anyway so at least he knows what I am talking about.*
*CALLER: Yeah, well, he would know, he would know where these things are coming from now. Now I don't know whether you would be briefed or whatever, but he is currently not even in the country, he is out of the country, he works out of the country, but he would, I know that well talking to my man in green, he is kind of saying, you know, that they would be proposing this particular individual."*

Shortly after the commencement of the Inquiry the Department of the Taoiseach passed to me a letter containing an unsolicited offer of assistance as an investigator from an individual whose CV indicated 20 years' experience in intelligence services as an officer in the Defence Forces. The offer was not taken up.

I was satisfied that the 'phone calls received by Mr [redacted] had not in fact influenced in any way his co-operation with the Inquiry. As these events had no bearing on the subject matter of the Terms of Reference I considered it unnecessary to investigate the 'phone calls further or to ascertain whether there was any connection between the assertions made by the caller and the above offer of assistance to the Inquiry.

# APPENDIX IV

AMX Touch Panel “Quick Start Guide” and specification from manufacturer’s website.

# APPENDIX V

Sunday Times Article 9th February 2014