Road Safety Camera Commissioner

INTERIM REPORT ON VIRAL INFECTION OF THE FIXED DIGITAL ROAD SAFETY CAMERA SYSTEM

Release date: 06 July 2017

TABLE OF CONTENTS

EXECUTIVE SUMMARY

1 This interim report is compiled in response to a request from the Minister for Police, the Hon Lisa Neville, to investigate *inter alia* the causes, effects, consequences and lessons from a malware infection found in the Victorian Fixed Digital Road Safety Camera System.

2 There is no evidence that the WannaCry infection has affected the integrity of Speed and Red-Light camera infringements.

3 I am satisfied that the mechanisms that construct and communicate the infringement data are unaffected by the virus.

4 I am satisfied that there is **no evidence** of any infringement data being in any way compromised.

5 I am satisfied that devices which measure and record speed are external to the infected computers and are unaffected by the virus.

6 I am satisfied with the accuracy and integrity of the infringements dated 6 June 2017 to 22 June 2017 (and thereafter).

7 I am satisfied that there is no evidence of any ongoing impact to the systems.

ACKNOWLEDGEMENT

This report has been achieved speedily thanks to many people and organisations who have generously shared their knowledge, their expertise, their data and their time. These include:

- Mr Stuart McCormack of ByteSmart Pty Ltd
- Department of Justice and Regulation
- Redflex Traffic Systems Pty Ltd
- JENOPTIK Australia Pty Ltd
- GATSO Australia
- SERCO Asia Pacific- Traffic Camera Services
- VIPAC Engineers & Scientists Ltd

PURPOSE

8 By communications on 22, 23 and 24 June 2017 the Minister for Police, the Hon Lisa Neville, requested me to investigate malware/ransomware virus infection in the Fixed Digital Road Safety Camera **(FDRSC)** network.

9 The purpose of this interim report is to provide a response relating to various urgent aspects of the investigation, and in particular:

- Which cameras across the Victorian Road Safety Camera System have been infected with the virus
- Whether there have been any infringements issued across the Victorian Road Safety Camera Network from 6/6/2017 that could be:
    - inaccurate as a result of the virus that should be withdrawn;
    - whether any damage may have been caused to the data held by any of the Victorian Road Safety Cameras as a result of the virus,
    - whether there has been any impact on the accuracy or reliability of the Victorian Road Safety Camera System,
    - whether there may be any future impact on the accuracy or reliability of the cameras as a result of the infection.

BACKGROUND

10 In Victoria, two independent **speed** measuring devices must agree within a tight tolerance before a potential infringement can be initiated. A manual check is carried out by two assessors, sitting independently. Further checks and balances exist to ensure the integrity and accuracy of the Road Safety Camera System.

11 In Victoria, where a potential red light infringement has been detected, the images recorded by the road safety cameras are scrutinised during manual processing by two assessors, sitting and assessing independently of each other. An infringement does not proceed unless they conclude that the images show the identified vehicle had entered the intersection or pedestrian crossing against a red light or red arrow.

12 *Ransomware* is a term used to describe a category of malicious software. The ***WannaCry*** ransomware virus/worm is a particular type of ransomware, which encrypts data on a computer and threatens to lock the owner out unless a payment is made. The Wikipedia pages are useful for introductory reading:

https://en.wikipedia.org/wiki/Ransomware ;

https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

13 WannaCry consists of three major components:

- A viral worm to spread the virus.
- An encryption system designed to deny users' access to their most valuable files.
- A communication tool to inform users, demand ransom and manage payment.

14 A number of variants of the virus exist.

15 The encryption component seeks out 'valuable' file types on the infected system (documents, email, spreadsheets, images, movies, etc.) and encrypts them. As part of this process, each file's extension is modified to reflect encryption; for example, *Doc1.docx* might be renamed *Doc1.docx.wncry.*

16 It is worth noting that most WannaCry variants make no further attempt to harm infected systems. To do so would be counterproductive; ransom cannot be paid from a disabled computer.

17 At some point prior to 7 June 2017, a variant of the WannaCry ransomware virus breached the perimeter of the Fixed Digital Road Safety Camera (FDRSC) network. The method of infection is yet to be determined.

18 Over the next ten days, the worm infected 43 Windows 7-based Redflex Camera Control Units (CCUs) and 67 Windows 7-based Jenoptik Site Controllers.

19 The infected systems continuously attempted to infect all other components of the FDRSC network. While there is no evidence that any further components were infected, the attacks appear to have caused systems based on older Windows variants to shut down intermittently

and inconsistently. Such behaviour- Windows XP crashing while under WannaCry attack - is consistent with test results published by security researchers.

20 Other than their attempts to spread the virus, the infected systems displayed no overt symptoms of viral infection.

21 The first indication of a problem was on June 6. Redflex noted that twenty Road Safety Camera detection systems on the Hume Highway had crashed.

22 Redflex began investigating the cause of the crashes. The investigation was hampered by the fact that the crashed (*affected*) systems were not themselves infected by the virus and displayed no symptoms other than seemingly random failures.

23 Over the next eight days Redflex undertook a series of steps to isolate the cause of the crashes.

24 On June 14 Redflex detected the WannaCry virus on a Windows 7-based Camera Control Unit. The Department of Justice & Regulation (DJR) was informed.

25 On June 16, Redflex informed DJR that the WannaCry virus had infected all of Redflex's Windows 7-based systems and that – apart from attempting to infect other connected systems – ***the virus had remained dormant.*** Redflex disinfected and inoculated all Windows 7-based Camera Control Units.

26 Also on June 16, Redflex tested the Microsoft patch for Windows XP systems (Microsoft Security Bulletin MS17-010). DJR gave approval to commence patching XP systems and also to scan the FDRSC network for additional infections. Three non-Redflex computers were detected to be attempting to spread the virus through the network. These were subsequently identified to be Jenoptik equipment.

27 On June 19, Jenoptik commenced scanning for and cleansing all infected machines.

28 On June 21, Jenoptik attempted to patch all infected machines. Two Site Controllers failed to patch correctly, and they were powered down and removed from the network. They were not turned back on. (They were replaced on June 27 with new hardware, which has been patched and are operational.)

29 By June 22 all infected systems had been patched. No further unusual behaviour has been noted.

SCOPE OF INVESTIGATION

30 This is the first part of the investigation requested by the Minister. With the expert assistance of the consultant Mr Stuart McCormack of ByteSmart Pty Ltd, my office arranged to identify which cameras were infected, whether the infringement data captured has been compromised, and whether there is any ongoing impairment of the integrity of the road safety camera system

RESULTS OF INTERIM INVESTIGATION

REDFLEX

31 The clocks on the infected machines are not used to calculate detected speed; such tasks are performed by dedicated subsidiary systems. Redflex have separately recalculated off-line all automatically generated speed detection data. One rounding difference (in favour of the motorist) was determined.

32 There is no evidence that the virus infection had any impact on the overall performance of the infected systems.

33 Redflex have demonstrated that the encryption component of the WannaCry virus failed to deploy. **There is no evidence of any encrypted files on any system**

34 To date, there is zero evidence of any viral impact on the accuracy or performance of these systems. There is **no evidence of any impact on the integrity of infringements.**

35 Redflex Camera Control Units which are based on older Windows variants were not infected by WannaCry infection. However, the repeated attacks by the malware resulted in the CCUs "crashing" periodically. Some of the machines stayed "crashed" but uninfected, others rebooted and resumed work without compromise of their integrity.

36 Redflex logging systems are transaction-based. If an action is not completed then the system rejects it. Thus, it is not possible for a partial or garbled infringement record to be created, even during a system failure.

37 I am satisfied that the detection systems maintain their integrity during a reboot. This is in line with the 2011 Auditor General investigation.

JENOPTIK

38 The Camera and Detection components of Jenoptik systems are Linux-based (not Windows based) and so were unaffected by the virus.

39 "Site Controllers" are computers used to translate Jenoptik data into camera logs and data of the kind required by the State of Victoria authorities. A total of 67 Jenoptik Site Controllers were found to be infected. These devices are dedicated to assembling Jenoptik's detection logs and associated data and with communicating the results to SERCO Traffic Camera Services.

40 There is no evidence that the encryption component deployed. There is no evidence of any impact on the integrity of infringements.

GATSO

41 GATSO Camera & Detection systems are Linux-based and were unaffected by the virus.

MOBILE CAMERAS

42 Mobile Camera and Detection systems have not at any time been connected to the Fixed Digital Road Safety Camera Network. There is no evidence that mobile cameras have at any time been exposed to the virus.

SERCO

43 SERCO report no evidence of unusual infringements, rates of infringement or rates of Excessive Speed Infringements arising from the FDRSC during the period of infection.

CONCLUSIONS

44 There is no evidence that the WannaCry infection has affected the integrity of Speed and Red-Light camera infringements.

45 I am satisfied that the mechanisms that construct and communicate the infringement data are unaffected by the virus

46 I am satisfied that there is **no evidence** of any infringement data being in any way compromised

47 I am satisfied that devices which measure and record speed are external to the infected computers and are unaffected by the virus

48 I am satisfied with the accuracy and integrity of the infringements dated 6 June 2017 to 22 June 2017 (and thereafter)

49 I am satisfied that there is no evidence of any ongoing impact to the systems.

RECOMMENDATIONS

50 I applaud the caution shown by the authorities, but I find that there is no reason for the subject infringements to continue to be withheld.