STATEMENT AND BACKGROUND MATERIAL IN SUPPORT OF MY COMPLAINT ABOUT UNLAWFUL COMMUNICATIONS INTECEPTION BY GCHQ IN VIOLATION OF S.1 OF THE REGULATION OF INVESTIGATORY POWERS ACT

This complaint arises from recent public disclosures that Government Communications Headquarters (GCHQ) has for some years engaged in a programme of indiscriminate and possibly unlawful access to, and storage of, webcam images of a substantial number – possibly millions - of Yahoo customers.

This programme – named “Optic Nerve” - was recently made public as a result of publication of a number of internal GCHQ documents made available by the whistleblower Edward Snowden.

If this information is verified it would be reasonable to conclude that GCHQ has engaged in unauthorised interception in violation of s.1 (1) of the Regulation of Investigatory Powers Act. This legislation provides for substantial criminal penalties, including imprisonment, for unlawful communications interception.

In this case, it would appear that the required s.42 RIPA authorisation was not issued by – or sought from - the Secretary of State. On the basis of the documentation it is doubtful whether any exemption (particularly the claimed “research” exemption) would apply to such a substantial interception operation.

As a user of Yahoo services, I – like many other people – have been deeply troubled by these reported mass surveillance activities. During the period of Optic Nerve’s operation I regularly used Yahoo services.

In light of 1) the circumstances set out in this letter, 2) the absence of an alternative complaint mechanism, 3) the existence of a substantial body of evidence and 4) the exceptional public interest in this matter, I request that you investigate this complaint as a matter of urgency.

Background to the webcam interception programme

On 28th February 2014 the Guardian newspaper reported that it had obtained documented evidence that GCHQ had indiscriminately intercepted and stored
the webcam images of a considerable number Yahoo! Messenger users.¹ The programme allegedly commenced operation in 2008 and remained active until at least 2012. Documents obtained by the Guardian explicitly state that a surveillance program codenamed Optic Nerve collected still images of Yahoo webcam chats in bulk and saved them to agency databases, regardless of whether individual users were an intelligence target or not. In one six-month period in 2008 alone, the agency collected webcam imagery – including substantial quantities of sexually explicit communications – from more than 1.8 million Yahoo user accounts globally.

A GCHQ internal memo confirming the project is set out in Appendix 1.

The system was used for experiments in automated facial recognition, to monitor GCHQ's existing targets, and to discover new targets of interest. Such searches could be used to try to find terror suspects or criminals making use of multiple, anonymous user IDs.

Rather than collecting webcam chats in their entirety, the program saved one image every five minutes from the users' feeds, partly to comply with human rights legislation, and also to avoid overloading GCHQ's servers. The documents describe these users as "unselected" – intelligence agency parlance for bulk rather than targeted collection. One document likened the program's "bulk access to Yahoo webcam images/events" to a massive digital police mugbook of previously arrested individuals.

**Substance of the concerns**

It may be useful to clarify the legal basis for an investigation of a s.1 RIPA violation by GCHQ.

- **Webcam data is content protected by RIPA**

  Webcam traffic falls within the definition of “interception” in s 2(2)(b) of RIPA:²

  (2) For the purposes of this Act, but subject to the following provisions of this section, a person intercepts a communication in the course of its transmission by means of a telecommunication system if, and only if, he—

  (a) so modifies or interferes with the system, or its operation,
  (b) so monitors transmissions made by means of the system, or
  (c) so monitors transmissions made by wireless telegraphy to or from apparatus comprised in the system,

as to make some or all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication.

- **A s.42 authorisation is required**

  S 42 (1) states that authorisations **must** be made by the issue of a warrant granted by the Secretary of State and must be compliant with s 32 of RIPA (s42(3)).

  Webcam traffic - if it shows people in their homes - is “intrusive” surveillance which must pass the tests of s 32 of RIPA. i.e. “necessary” (s 32(2)), “proportionate” (s 32(3)) and for the purposes set out in s 33: “in the interests of national security; for the purpose of preventing or detecting serious crime; or in the interests of the economic well-being of the United Kingdom.”

- **The claimed research exemption is invalid**

  In these circumstances a claimed research justification could not meet the necessity and proportionality tests. If technical testing of face recognition algorithms were considered “necessary” via webcams it could have been undertaken in a controlled environment, indeed the research would be more valid because a variety of test circumstances could be established.

**RIPA protections are relevant regardless of the location of target individuals.**

  RIPA and ISA appear to be agnostic as to territoriality (though enforcement would generally take place via UK mechanisms). However the question of territory is largely irrelevant. GCHQ accessed images substantially via a UK public telecommunications system, and in the case of webcam images of overseas targets in conversation with UK residents the access would also involve intercepting private systems.

  These circumstances indicate that a s.42 authorisation would most definitely be needed to lawfully conduct the interception. On the basis of the published documentation, however, it would seem that such authorisation was neither sought nor granted.

  One internal document explained the agency’s reasoning:

  "It was agreed that the legalities of such a capability would be considered once it had been developed, but that the general principle applied would be that if the accuracy of the algorithm was such that it was useful to the
Complaint concerning s.1 RIPA violation by GCHQ

"The number of spurious results was low, then it was likely to be proportionate."

"This is allowed for research purposes but at the point where the results are shown to analysts for operational use, the proportionality and legality questions must be more carefully considered."

This assessment demonstrates a fundamental misunderstanding of the law. RIPA criminalises the “fact” of an intercept unless at least one of a limited number of conditions has been met. How the intercepted data are processed - or the purposes to which they are put - are not relevant.

It is possible that staff had failed to differentiate between the permissible exemptions and exceptions in RIPA and the Data Protection Act (1998) (DPA) and had confused the two pieces of legislation. Certain research purposes are permissible under the DPA. However, even if this exemption was relevant, the DPA does not in any practical sense apply to GCHQ. Even if a full exemption for research existed under the DPA this condition would have no bearing on the authorisation requirements set out in RIPA.

It is also important to consider the possibility that SoS authorisation was sought and obtained, but that the SoS acted ultra vires, issuing a warrant outside the scope permitted in RIPA, perhaps on poor legal advice. This situation may fall within the scope of other investigatory entities for consideration, or even be subject to judicial review.

**Inadequacy of alternative complaint mechanisms**

The Data Protection Act (1998) has limited relevance to GCHQ’s activities. Most of the key principles (particularly the 1st, 2nd and 8th principles) are exempt, while the 3rd and 5th principles have almost no effect. The extensive use of s.28 certificates has created a default exemption for national security operations.

The absence of a s.42 authorisation is most likely a procedural failure by GCHQ rather than a breach of responsibility by the Secretary of State, and so this issue would not be of relevance to either the Interception of Communications Commissioner nor the Investigatory Powers Tribunal.

Additionally, in instances of alleged criminal law violations, neither the Commissioner nor the Tribunal will take action on complaints. Instead, they advise that the matter should be brought to the attention of police.

The option of approaching the Parliament’s Intelligence and Security Committee is theoretically available, however the terms of reference of the committee’s
present inquiry\(^3\) are more focused on the adequacy of the legal framework rather than an investigatory approach to specific operational issues.

\(^3\) https://b1cba9b3-a-5e631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20131017_ISC_statement_privacy_and_security_inquiry.pdf?attredirects=0
APPENDIX 1

SECRET STRAP1

Reference: B/7199BA/5001/5/114
Date: December 2008
Copy no:
Issued by: B18, GCHQ

OPTIC NERVE – Yahoo Webcam display and target discovery

Summary
A report on the development of OPTIC NERVE – a web interface to display Yahoo Webcam images sampled from unselected intercept and a system for proportionate target discovery

Metadata:
• At the moment OPTIC NERVE’s data supply (run by B13) does not select but simply collects in bulk, and as a trade-off only collects an image every 5 minutes. It would be helpful to incorporate selection and collect images at a faster rate (all?) for targets. CS to find out from B13 if this is feasible.

Source: The Guardian newspaper