NO CCTV
www.no-cctv.org.uk
info@no-cctv.org.uk
T: 07746 900645

PRIVACY INTERNATIONAL
www.privacyinternational.org
privacyint@privacy.org

12th January 2011

Mr Christopher Graham
Information Commissioner
The Office of the Information Commissioner,
Water Lane,
Wycliffe House,
Wilmslow, Cheshire SK9 5AF
UNITED KINGDOM

Dear Mr. Graham,

Complaint: Internet Eyes

We are writing further to our October 2009 complaint with regards to the "Internet Eyes" system that has recently been trialled by the UK company Internet Eyes Ltd.

In your response of April 2010 you stated that you could not issue an Enforcement Notice to prevent a new service from starting up. Now that the service has been started up as part of a three month trial we urge you to re-consider our original concerns along with further concerns laid out herewith.

It is still our view that Internet Eyes violates the Data Protection Act and we would ask that you take action to stop the full scale launch of the service which would in our view set a worrying precedent.

Our October 2009 complaint laid out specific breaches of the Act with reference to the Act's principles. We are aware that the CCTV Code is, as you pointed out, "guidance rather than express legal requirements" - this is why we only used the CCTV Code to illustrate breaches of the core principles. That said, if the CCTV Code is deemed so irrelevant then it does rather bring into question the purpose of the Code.

Retention and distribution of personal data

In our complaint we asked "What is to stop an internet viewer of the Internet Eyes system taking a screen grab or videoing images from a CCTV feed and then keeping those images permanently and distributing them as they see fit?" You assured us that Internet Eyes Ltd had told you "that disabling the print screen and right click functions at the viewer's end will guard against footage 'leaking out'." The trial of the Internet Eyes service

has shown that this unlikely claim was, as we suspected, impossible. We have located two leaked videos on the YouTube website which demonstrate that Internet Eyes Ltd has failed to prevent such leaks. The videos can be found at the following web addresses:

1. http://www.youtube.com/watch?v=GsI6MGpRmiE
2. http://www.youtube.com/watch?v=x6wV7pHFZyE

In the first video, a customer in the feed on the left is clearly identifiable as he leaves the shop about 1 minute 30 seconds into the video.

Principle five of the Act states:

> "Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes".

When a visitor to the YouTube website views a leaked video then a copy of that video is created in the cache of the web browser and stored on the user's hard drive. Furthermore programs exist that can be used to download video from YouTube. In light of this it is possible for personal data to be retained indefinitely. Principle five is therefore breached.

Principle seven of the Act states:

> "Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data".

Clearly appropriate technical and organisational measures have not been taken as personal data has been leaked to the YouTube website and Internet Eyes does not therefore comply with principle seven.

Principle eight of the Act states:

> "Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data".

When data is available over the internet on websites such as YouTube there is no control on which country the data is transferred to and so Internet Eyes does not comply with principle eight.

As we stated in our October 2009 complaint, even if Internet Eyes Ltd manage to prevent screen capture (and we contend that it is unlikely they ever could), then it is still possible for an Internet Eyes viewer to record a CCTV stream using a video camera.

Section 29(1) exemption and the adjective "necessary"

In your response of April 2010 you did not address our concerns with regards to "necessity" – namely the requirement in Schedules 2 and 3 of the Act which states that the processing of personal data must be "necessary" for the purposes pursued by the data controller (in this case presumably "for the administration of justice") .

We maintain the view that transmitting images over the internet in a way that cannot be controlled (see 'Retention and distribution of personal data' above) and whose role in the “administration of justice” is tenuous at best, cannot be argued as “necessary”. Therefore we hold that Internet Eyes cannot rely on the Section 29(1) exemption relating to “the administration of justice”.

Though no explicit definition of “necessary” appears in either the Act or the underlying EC directive (Directive 95/46/EC), Schedule 2 paragraph 6(1) of the Act states:

> The processing is **necessary** for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, **except** where the processing is unwarranted in any particular case because of prejudice to the rights and freedoms or legitimate interests of the data subject.

The Data Protection Act is underpinned by Article 8 of the European Convention on Human Rights. From this underpinning we can glean a definition of “necessary” as laid out in case law – specifically Silver-v-UK [1983] ECHR 11 and Handyside-v-UK (1976) 1 EHRR 737, 1 EHRR 737, (1979) 1 EHRR 737, [1976] ECHR 5, [1976] ECHR 5493/72. The Silver judgment states:

> the adjective "necessary" is not synonymous with "indispensable", neither has it the flexibility of such expressions as "admissible", "ordinary", "useful", "reasonable" or "desirable" (see the Handyside judgment of 7 December 1976, Series A no. 24, p. 22, § 48);

Clearly the word “necessary” is open to some interpretation but we have yet to see any explanation of why the Internet Eyes system is deemed “necessary” for the administration of justice. Furthermore, even if it were possible to make an argument for its “necessity”, we submit that identifiable images of customers going about their lawful daily business being leaked onto the internet cannot be other than prejudicial “to the rights and freedoms or legitimate interests of the data subject”.

Responsibilities of the Data Controller

It is our understanding that Internet Eyes Ltd and the shopkeepers that have installed Internet Eyes are joint Data Controllers. As such, what steps will Internet Eyes Ltd and the shopkeepers take to protect the freedoms and legitimate interests of data subjects in accordance with Schedule 2, paragraph 6(1) of the Act? Are shopkeepers made aware of the additional burdens that will be placed upon them when operating CCTV over the internet as is the case with Internet Eyes? The shopkeeper may have additional information that combined with CCTV images could be used to fully identify customers, such as credit card details or name and address for deliveries – this further increases both the sensitivity of the personal data in question (the CCTV images) and the shopkeepers' responsibility to the data subjects. Do shopkeepers understand that they are not outsourcing their data protection responsibilities?

Identifiable individuals

You told us that Internet Eyes would take steps to avoid data processing in breach of the Data Protection principles by: “reducing the possibility that any of the footage streamed to viewers will contain images of identifiable individuals”. This would be achieved by the

following:

1. Viewers will only see images for a relatively short time, they receive four streams at once and one of these is replaced every five minutes;
2. The streams provided are selected at random and none will be within the postcode area of the viewer;
3. Shopkeepers will be advised on the siting of cameras to avoid giving away the location of the premises

Furthermore, you stated that “IE place a great deal of weight on the fact that the images are small and of low quality. Colleagues who have viewed examples confirm that this is the case and that although the footage might be good enough for viewers to spot a possible incident it is unlikely to be good enough to recognise faces. As a result, it is even more unlikely that an individual could be identified from the footage by a viewer who only sees footage containing a grainy image of that individual once and for a short time.”

In the first leaked video listed above the shop customer being filmed is clearly identifiable, as is the shop. We have been contacted by people who have been able to identify the location of the leaked CCTV feeds. The location of one of the feeds can also be identified through media reports of the system.

Clearly whatever measures Internet Eyes Ltd put in place were ineffective. Even point 2 above is weak protection of personal data. What is to stop a viewer registering at one postcode but using a computer in another postcode? Even if the feeds are not leaked onto the wider internet, limiting feeds to the postcode of a registered address is not a guarantee that a viewer will only view feeds outside their locality.

Fair processing and consent

We contest that Internet Eyes cannot rely on the Section 29(1) exemption as stated above and therefore must be bound by the consent requirement under both Schedules 2 and 3. Customers must be clearly informed that the protection of their personal data is at risk and they must have a clearly defined opportunity to make an explicit choice. We note that the signage used by Internet Eyes reads as follows:

> “Images are being monitored for the purposes of crime and public safety. CCTV images from this shop are viewed by people working away from these premises. Live footage for the Viewers is made available 24hrs a day by Internet Eyes Ltd.”

As well as the above text, the words “Internet Eyes” are displayed along with the Internet Eyes logo. Whilst it could be argued that the fact that images are viewed over the internet is implied by the company's name it is not explicitly stated. Customers cannot therefore give informed consent to the system as they are not properly informed of what it is. In light of the leaked videos (as described above) the signs would have to make it clear to customers that anyone anywhere may be able to view the images.

Dual role of the ICO

We are concerned that the dual role of the Information Commissioner's Office as both enforcer of breaches of the Act and advisor to Data Controllers on how to comply with the Act creates a conflict of interest that has affected the way that the Internet Eyes system has been assessed. Since the initial announcement of the Internet Eyes system we are aware that the ICO worked with Internet Eyes Ltd, advising them on how to meet

requirements for compliance with the Act. When groups such as ours issue complaints about the Internet Eyes system it seems odd that the official channel for such a complaint is the body that is advising Internet Eyes Ltd on compliance.

We are sure that you would agree with us that the ICO's role is primarily to protect personal data rather than to advise companies how to squeeze between the gaps in privacy protection. We hope that you will seriously consider the breaches of the Act that we have outlined above and look forward to your full response to all our concerns.

Yours sincerely,

Simon Davies, Privacy International

Charles Farrier, NO CCTV