PRIVACY INTERNATIONAL

265 Strand
London, WC2R 1BH, GB

T +44 (0)208.123.7933
privacyint@privacy.org

www.privacyinternational.org

27 October 2009

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

Complaint: Internet Eyes

Dear Mr Graham,

We are writing on behalf of a number of people who have complained to No CCTV and Privacy International with regard to the "Internet Eyes" system that the UK company Internet Eyes Ltd plans to launch next month and for which they have already begun recruiting "viewers" and "customers".

It is our view that Internet Eyes violates the Data Protection Act and we ask that you take immediate action to prevent the launch of this service and the encroachments on the core principles of the Act that would ensue. Internet Eyes is described as *"an online instant event notification system"*. Using 'Open Circuit Television' (OCTV) software, viewers watch random live CCTV feeds over the internet from UK businesses subscribed to the service with the promise of cash rewards for viewers that spot the most crimes.

The Information Commissioner's Office (ICO) CCTV code of practice lays out recommendations which are based on the enforceable data protection principles under the Data Protection Act 1998, Schedule 1. Our concerns are as follows:

- Section 29(1) of the Data Protection Act exempts personal data processing from the first data protection principle when such processing is for the prevention, detection or resolution of crime. However Schedules 2 and 3 state that the processing must be "necessary" for this purpose. We submit that transmitting images over the internet in a way that cannot be controlled (as expanded upon below) cannot be argued as necessary. Exemptions relating to "the administration of justice" are not a license to be reckless with personal data. We submit that Internet Eyes does not pass the test of necessity.

- In light of the fact that Internet Eyes cannot rely on the exemption stated above, the project must be bound by the consent requirement under both Schedules 2 and 3. There is some debate about what constitutes consent but at the very least people 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.

- It is not possible for someone to consent to something about which they are not properly informed. The EU Data Protection Directive defines consent as: *"…any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed"*. The ICO 'Data Protection Act 1998 Legal Guidance' points out that: *"The fact that the data subject must "signify" his agreement means that there must be some active communication between the parties."* In the ICO's CCTV code of practice, Section 9.1 'Letting people know' is no longer simply guidance but a basic requirement. It states: *"Signs should: be clearly visible and readable; contain details of the organisation operating the system, the purpose for using CCTV and who to contact about the scheme (where these things are not obvious to those being monitored);"* It goes on to state: *"Signs do not need to say who is operating the system if this is obvious. If CCTV is installed within a shop, for example, it will be obvious that the shop is responsible."* Evidently in the case of a shop CCTV system connected to the Internet Eyes system it would not be clear who is responsible for the system. Signs would have to be placed outside any shop or business that any images of data subjects could be viewed on the internet and that it is not possible to control who views these images or how they may be distributed. Not displaying such signs would be unacceptable. Furthermore, this breaches of the fairness requirement in the first principle.

- Principle two of the Data Protection Act states: *"Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes".* The ICO guidelines in relation to this principle are expressed in the CCTV code of practice, Section 8.2 'Disclosure' which states: "If the system is established to help prevent and detect crime it will be appropriate to disclose images to law enforcement agencies where a crime needs to be investigated, but it would not be appropriate to disclose images of identifiable individuals to the media for entertainment purposes or place them on the internet." Internet Eyes Ltd have no way of knowing who is viewing their images and as described below they have no way of controlling where such images are stored or distributed. In fact, they are expressly disclosing images of identifiable individuals for entertainment purposes and placing them on the internet.

- Principle five of the Data Protection 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"*. The ICO guidelines in relation to this principle are expressed in the CCTV code of practice, Section 8.3 'Retention' which states: *"You should not keep images for longer than strictly necessary to meet your own purposes for recording them."* 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? Operating cameras over the internet in this way will mean that there will be no way of restricting retention of images.

- Principle seven of the Data Protection 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"*. The ICO guidelines in relation to this principle are expressed in the CCTV code of practice, Section 10 'Staying in control' which states: "All images must be protected by sufficient security to ensure they do not fall into the wrong hands. This should include technical, organisational and physical security. For example: Are sufficient safeguards in place to protect wireless transmission systems from interception? Is the ability to make copies of images restricted to appropriate staff? Where copies of images are disclosed, how are they safely delivered to the intended recipient? Are control rooms and rooms where images are stored secure? Are staff trained in security procedures and are there sanctions against staff who misuse CCTV images? Are staff aware that they could be committing a criminal offence if they misuse CCTV images?" Short of creating a new security structure for the entire internet it is not possible for CCTV images transmitted via the Internet Eyes to be "protected by sufficient security to ensure they do not fall into the wrong hands". As described above it is simply not possible to control the viewing, storage, retention or redistribution of images. Internet Eyes has not made any plans clear regarding the necessary training of Internet viewers of this service in security or any other procedures relating to CCTV.

- Principle eight of the Data Protection 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"*. On the basis of ICO advice (for example in the CCTV Code of practice) anything that can be used to identify a person, whether by way of facial characteristics or other qualities, clothing or behaviour, constitutes personal information under the Data Protection Act. As has been explained above it will not be possible to control the viewing, storage or retention of images viewed over the internet and so it will not be possible to prevent the transfer of personal data to countries without an "adequate level of protection of the rights and freedoms of data subjects".

It may be claimed that many of the above issues can be cast aside by simply transferring the data protection responsibilities to Internet Eyes viewers, but the nature of the internet does not make this possible. The internet quite rightly was designed without the need for excessive amounts of user authentication. Internet users can also use anonymous proxies and other such technologies to shield their identity – again, quite rightly. As a result it will not be possible to verify the identity of Internet Eyes viewers. Even where a reasonable degree of certainty about identity can be assumed it is impossible to control who, other than the reg-

istered viewer, views the images short of installing cameras in the home of every user of the system.

The complaints that we have received in relation to Internet Eyes have expressed concerns about privacy in a far more wide reaching manner than the principles laid down in the Data Protection Act and we share the view of Desmond Browne QC, Chairman of the Bar Council, that in a country with a strong common law tradition it is the common law principles which govern protection of our privacy that we should all be working to uphold. In the meantime we hope that the Data Protection Act will hold as a first line of defence and prove strong enough to protect us from Internet Eyes and the very serious consequences of allowing this latest attempt to expand surveillance in Britain.

Sincerely yours,

Simon Davies, Privacy International

Charles Farrier, NO CCTV