IN THE INVESTIGATORY POWERS TRIBUNAL Case No IPT/13/92/CH

BETWEEN:

PRIVACY INTERNATIONAL

Claimants

-and-

(1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS
(2) GOVERNMENT COMMUNICATION HEADQUARTERS

Defendants

WITNESS STATEMENT OF IAN BROWN

I, Ian Brown, Senior Research Fellow and Associate Professor, Oxford Internet Institute, University of Oxford, One St Giles, Oxford OX1 3J, United Kingdom, SAY AS FOLLOWS:

1. I write in support of Privacy International's claim in this matter. I rely on an early statement that was written by me in support of the Applicants in the matter Big Brother Watch, Open Rights Group, English PEN and Dr Constanze Kurz v United Kingdom, Application No: 58170/13 ("BBW application") in the European Court of Human Rights and the exhibits referred to therein. Documents referred to in this statement are exhibited marked "IB/1."

2. The BBW statement was made on 27 September 2013, and it continues to represent my best understanding of the communications surveillance activities of the UK government.

3. Since September 2013, allegations of a number of further GCHQ activities have been made by the media, based on the documents leaked by ex-NSA contractor Edward Snowden. Further details have also been revealed of the

UK's intelligence oversight regime. Based on my broader understanding of the technology and legal framework covering such activities, I believe the following are most relevant to Privacy International's claim:

a. GCHQ monitoring of millions of video calls made by Yahoo! users (Operation OPTIC NERVE). The sensitive nature of these calls is highlighted by claims that GCHQ was required to institute a programme to limit officials' access to around 7 per cent of images stored, which contained "undesirable nudity". The proportionality of this programme is questionable– in the words of US Senators Ron Wyden, Mark Udall and Martin Heinrich, demonstrating a "breathtaking lack of respect for privacy and civil liberties".[1]

b. The cursory nature of the Intelligence Services Commissioner's investigation into the legality of the conduct described by the Snowden revelations, which was a "surprise" to the House of Commons' Home Affairs Committee.[2] More broadly, I would support the Committee's conclusion that "current oversight is not fit for purpose" (§145) – neither in the structure or operation to date of the reformed Intelligence and Security Committee; nor in the resources and time available to the Intelligence Services and Interception of Communications Commissioners.

c. The large-scale access to Google and Yahoo!'s internal data flows obtained by the joint National Security Agency and GCHQ Operation MUSCULAR, despite the NSA's statutory powers to obtain data from US service providers in a more targeted way.[3]

4. I was surprised to read in the UK government's response to Privacy International's claim that they considered messages between UK users of services such as Facebook to be "external" communications that can be accessed in bulk under s.8(4) of the Regulation of Investigatory Powers Act. As Jemima Stratford QC and Tim Johnston stated in their Opinion for the All-Party Parliamentary Group on Drones, such an interpretation is "an artificial construction, which does not reflect the language or intention of the statutory framework." It is not in my view supported by the Interception of Communications Code of Practice, case law of the Court of Justice of the European Union, or ministerial statements in the House of Lords during the passage of the Act.[4]

---

[1] Spencer Ackerman, Senators to investigate NSA role in GCHQ 'Optic Nerve' webcam spying, *The Guardian*, 28 February 2014

[2] Seventeenth Report, *Counter-Terrorism*, 30 April 2014, §164

[3] Sean Gallagher, How the NSA's MUSCULAR tapped Google's and Yahoo's private networks, *ars technica*, 31 Oct 2013

[4] *In the matter of state surveillance*, §§19-24, at http://www.tom-watson.co.uk/wp-content/uploads/2014/01/APPG-Final.pdf

5. I must also emphatically disagree with the statement of the Interception of Communications Commissioner, quoted in section 118 of Mr Farr's witness statement, that "intrusion…into the privacy of innocent persons would require sentient examination of individuals' communications." The contrary has for decades been the position of the European Court of Human Rights. In *Klass v Germany*, that Court stated:

> *"[A] system of surveillance under which all persons in the Federal Republic of Germany can potentially have their mail, post and telecommunications monitored, without their ever knowing this unless there has been either some indiscretion or subsequent notification in the circumstances laid down in the Federal Constitutional Court's judgment…directly affects all users or potential users of the postal and telecommunication services in the Federal Republic of Germany…this menace of surveillance can be claimed in itself to restrict free communication through the postal and telecommunication services, thereby constituting for all users or potential users a direct interference with the right guaranteed by Article 8."*[5]

6. An automated system such as TEMPORA creates a similar "menace" for all Internet users, who (without further leaks) are not in a position to discover whether their communications have been collected; picked out using automated analysis; or as a result been examined by a human being. The privacy intrusion does not occur only at the end of that chain.

7. I hope you find this information useful in your consideration of Privacy International's claim.

STATEMENT OF TRUTH

I believe that the facts stated in this witness statement are true.

SIGNED Ian Brown.....

Ian Brown

DATED: 7/6/14.....

7 June 2014

[5] App. No. 5029/71 s.37