To: Intelligence and Security Committee of Parliament
From: Barbara Moore
Data: 7 February 2014
Subject: Privacy and Security Inquiry - Call for Evidence

About me: I am a private individual, sole trader: internet marketing, web development and website hosting. In 2009 I gave oral evidence before the apComms inquiry into internet traffic - 'Can we keep our hands off the net?' Since then I have become more interested in what happens over the internet and the interaction between the general public and the hidden threats to privacy and security posed by the internet. In particular, campaigning against the use of deep packet inspection (DPI) systems for commercial profit.

Before I begin may I voice my concerns over the methods used by this Inquiry.

1. Use of Word format for emailed response. This suggests very poor advice to the Committee. Word format is renowned as at least a major cause of Windows computers crashing and at worst carrying 'bad' scripts. I regret I do not have any software that outputs Word format so send my submission as plain text. I trust this is acceptable to you.

2. The use of Google's servers to host the PDF document outlining the Call for Evidence. Here I have two concerns about advice given to the Committee.

2.a. Google hosting is part of the worry regarding NSA surveillance (along with any other USA based corporation or international business with a US branch)

2.b. PDF format is renowned for being infected with 'bad' scripts.

3. As the methods used show scant regard for the concerns of the public how can anyone think that this is a serious inquiry?

There end my concerns. Below I submit my evidence.

Regards
Barbara Moore

Evidence Summary: There is a complete mis-match between how the current laws are being enacted and the publics' perception of the ways in which the various data collection and interception laws protect them. There is growing evidence that interception is both out of control and ineffective and that those who the public expect to have oversight are themselves unaware of what is going on; whether parliamentary or judiciary oversight.

a) What balance should be struck between the individual right to privacy and the collective right to security?

How does this differ for internet communications when compared to other forms of surveillance, such as closed-circuit television cameras? To what extent might it be necessary and proportionate to monitor or collect innocent communications in order to find those which might threaten our security? How does the intrusion differ between data (the fact a call took place between two numbers) as opposed to content (what was said in the call)?

1.1 As a hoster of websites and mail servers I am very aware of the need for security over the internet. However, as a host I also see through the various access logs how many replay attacks follow the visitors to my websites. My efforts to protect my visitors and the intellectual property on hosted sites are worth nothing if DPI systems and interception taps are also being used to harvest the communication data of visitors. There is little difference between the 'meta data', traffic data and content harvesting: all undermine the commercial value of the websites and destroy any privacy of the communication between site visitors and site owners.

1.2 It is all a matter of trust. If you are enjoying a private conversation and someone appears to be listening you will either stop the conversation or move off to where you can continue the conversation in private. For a while websites used encryption to protect the conversation. However the Snowden revelations have exposed the ease with which encryption has been broken and MITM (man-in-the-middle) attacks have become common place through the activities of NSA, GCHQ and other nations' security services.

1.3 The effect of surveillance has resulted in a shift from the relatively simple task of protecting internet communications from criminal, RU (Russian) and CN (Chinese) hacking efforts to realising that there is no possible means of offering any security over the internet. It is a very sad end to an open system which was doing much to remove borders and to facility collaboration between people living anywhere on this planent.

1.4 To consider a comparison with a visible presence of closed-circuit television cameras is meaningless. Rather the comparison should be with the postal service, telegraph, telephone and facsimile and the expectation of privacy that has been part of the law since the early days of these services.

b) Whether the legal framework which governs the security and intelligence agencies' access to the content of private communications is 'fit for purpose', given the developments in information technology since they were enacted.

2.1 A reading of the various statutes appears to offer sufficient protections. However the reality has revealed that the written words are not being taken with their common meaning. It was difficult enough to read that private conversations between solicitors and their clients where being recorded and used as evidence because a clause in RIPA is used to override other statutes. [http://www.publications.parliament.uk/pa/ld200809/ldjudgmt/jd090311/mce-5.htm]

2.2 Another example of the failure of statute is the complete omission of any investigation relating the the BT/Phorm use of DPI; the ongoing use of interception by TalkTalk with their Chinese partner, Huawei; mobile phones sharing location data with advertisers; BT sharing traffic data with Hitwise, the UK Government sharing data with Google, Facebook and other commercial corporations ... the list goes on and on.

2.3 The public were already tired of having the private conversations with websites intercepted by commercial entities. Discovering that the UK Government is active in allowing foreign security services to harvest this data and more destroys the last possibility of any faith in protections offered to citizens by statute.

2.4 The public can no longer trust any means of communication. Not even a face-to-face conversation in the privacy of their own homes because of the ability of mobile phones to eavesdrop even when turned off.

c) Proposals for specific changes to specific parts of legislation governing the collection, monitoring and interception of private communications.

3.1 Legislation is so lacking in 'fit for purpose' that there seems little point in doing anything other than repealing it and starting again from scratch. From news reports it would appear that Germany is a leader in 'best practice'. Perhaps it takes a nation that has lived through a period of monitoring by invisible services to place a value on privacy and freedom from constant monitoring by the state. Has Britain forgotten its recent history and the thousands who fled or lost their lives because of their beliefs? If Arthur Miller wrote his play today, how would it compare to 'The Crucible' written in 1950s America?

3.2 It is difficult to see from what all the constant monitoring is designed to protect us. It did nothing to protect one man from being attacked by murderous criminals. It did nothing to protect our children from coming home from school that day to tell us that someone had been beheaded. It did nothing

to protect the general public from broadcasts showing a dead man lying in the street and men with blood on their hands. The innocents became witnesses and will carry the images for the rest of their lives. Every one of the thousands of flowers left in tribute along the roads in Woolwich should serve as a reminder of the priorities of the public.

3.3 The current monitoring of digital traffic by international security services is a complete failure. It does nothing to protect UK e-business from criminal activity. Hack attempts against web hosts are as successful as ever. Infections of computers through visiting websites hosting malware is on an increase. Spam from customers of UK ISPs that are part of a botnet is as high as ever. In the physical world, gangs are spreading their influence and illegal trade around the country while money laundering is common place.

3.4 There is a need for evidence to be gathered. The collection needs to be proportionate. It needs to have the support of the public. There is no need for a law for one medium of evidence and a different law for a different medium. For as long as a few people 'in charge' can decide on secret surveillance without judicial oversight and full disclosure after the event including whether or not criminal evidence was collected there can be little trust in the process.

Conclusion:

4.1 Surveillance law is broken and been patched to the point of being dangerous to the freedom, democratic rights and civil liberties of the current and future generations.
4.2 The Britsh public and businesses should have confidence that the security services will protect their communications from surveillance by foreign entities: corporate or government sponsored, not collude in the invasion of privacy and corporate spying.
4.3 Whistleblowers who expose the excesses of surveillance should be offered full immunity and be treated as national heroes for protecting our society.