To: Intelligence and Security Committee of Parliament

Privacy and Security Inquiry – Call for Evidence

Submission by Miles Golding, private individual

I am a self-employed musician and violin teacher who has worked in this field in the UK since 1973, and am pleased to have the opportunity to submit my thoughts to the ISC for your consideration.

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

1. Every individual has the right to privacy unless there is compelling evidence that he or she might commit a crime. If that possibility is judged to be real and serious by an appropriately qualified professional, then warrants must be applied for and issued by an appropriately qualified legal officer.

2. Collecting terabytes of private information, including information about wholly law-abiding citizens, can lead to horrifying powers that, sooner rather than later, will be exploited by someone who has their own interests at heart rather than the so-called collective security of the nation. In other words, abuse of the system. Try as you might, you cannot pro-actively plug all the potential leaks. We know that corruption exists to an unacceptably wide extent within the Police Force, and the forces that tempt bent coppers to act illegally and collude with criminals outside the Force will likewise tempt some within the companies and/or government departments that will administer such data to access personal information for their own nefarious and selfish purposes. We also know how we cannot rule out human error and frailty, as evidenced by large data leaks from lost flash drives and laptops. Already we know that GCHQ has illegally passed data about UK citizens – and presumably companies alike – to their chums in the NSA. And no doubt some of those chums in the NSA will feel it is their duty to compromise the confidentiality of sensitive UK corporate material and pass it on for the benefit of US competitors, just as Snowden felt it was his duty – and rightly so – to reveal those terrifying secrets. The possibility of leaks is far too real for comfort.

3. You must consider too the **corporate** right to privacy. We know that back doors are built into routers and other hardware. Such devices must be strictly controlled and legislated against. Through such means and through hacking of data storage drives, corporate secrets, and even government secrets, can so easily fall into unfriendly hands, thereby threatening a nation's economy and political stability. For many years we have seen security failures in government and other sensitive websites caused by the hacking of databases and leaking of data through poor software design and/or maintenance. Our government seems quite happy to sell out to their corporate masters in Google, BT, and all those commercial organisations that reap personal data on every visit we make to a government website. Unfortunately few MPs and civil servants seem to understand the complexities of the technology, and companies have been able to blind the law-makers and the decision-makers with even simple science and bamboozle them into acceptance.

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. All communications should be judged the same, whether it is a letter in an envelope delivered by Royal Mail or an email. It just happens to be very easy to eavesdrop on telecommunications, particularly those involving text, hence the rapid rise in intrusive surveillance and gathering of data that companies then misuse to learn about individual habits and behaviour. This will lead to an increasing sense of unease amongst individual citizens, and they will learn to distrust even the most benign and well-meaning company, doctor's surgery, supermarket, mobile phone app, and website that has warnings about cookies. They will block everything rather than risk trusting it, and retreat to a world where the eyes of Google, GCHQ *et al* can not pry. I will be writing to my GP to say that I wish to opt out of care.data. I just don't trust this government, these civil servants and my NHS Trust to get it right. I have no apps on my smartphone – Twitter, BBC Weather for example – that I will not load because I do not trust them. So all this wonderful technology is wasted because successive governments have been caught napping and have betrayed its citizens by failing to protect their privacy adequately, and have instead fed the hands of their corporate masters, and no doubt enjoyed a few backhanders in return.

2. You must not create a smokescreen of the "anonymising" of personal information. We know that this can be very easy to subvert. "Anonymous" details can be pieced together very easily to pinpoint an individual. Metadata can be analysed – and you are disingenuous to define "data" as opposed to "content" as being merely"the fact a call took place between two numbers". The recent Petraeus scandal emerged mainly through the analysis of metadata. There is more than just telephone numbers in such data; you should know that, and appear to reveal ignorance – just how many really skilled experts are advising you, and just what are their credentials? I hope that the government's breadth of knowledge has increased from the not so distant embarrassment of a Minister thinking that an IP address referred to Intellectual Property.

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.

1. The legal framework that governs offences should be fit for purpose, but has been overridden, and abused by successive governments. The internet activity of me and the rest of my family, and thousands of other BT customers was secretly intercepted by BT in 2006/2007 in collaboration with a company called Phorm, a clear offence under RIPA, yet the government and the Police and the CPS colluded and made feeble excuses not to prosecute the offenders, although they were quite happy to jail people like Mulcaire and Goodman for the same offence against RIPA. Feeble excuses such as "they acted in good faith" "it was an honest mistake" and "is unlikely to be repeated" were used to justify the lack of prosecution. If I were to use such a defence before a judge and jury I would be laughed out of the courtroom. David Cameron has made much of the "Big Society" and being strongly against a "them and us" society, yet here we have the chums in big business cosying up to their chums in government and the civil service, and turning a blind eye when one of the chums breaks the law.

2. There are further instances of such sanctioning of serious law-breaking. It is now known that GCHQ carried out DDOS attacks against civilians, an offence for which civilians, such as Jake Davis, have been severely punished. Again, a shocking example of the them-and-us society in action. Those senior figures in GCHQ who sanctioned that, as well as the illegal passing of illegally-gathered telecommunications information to the NSA, should be prosecuted.

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

1. Increase the penalties, ensure that the Law is applied without fear or favour, and ensure that the Police and the CPS are transparently autonomous, and answerable to a properly autonomous authority. UK Justice services have betrayed the trust and faith of UK citizens.

2. Our society is under a far greater threat than international terrorism; that is the threat of distrust and alienation that arises from an increasing level of perceived corruption and arrogance in our government, civil service, police forces and security establishments such as GCHQ, that saw those 2011 riots emerge. This and successive governments must restore public trust and comfort, otherwise I fear further erosion of those precious democratic values that we all should hold dear.

Miles Golding

6 February 2014

[REDACTED]