[REDACTED]

Privacy & Security Enquiry
Intelligence & Security Committee of Parliament
35 Great Smith Street
London
SW1P 3BQ

18 January 2014

Dear Sirs

Privacy & Security Inquiry – Call for Evidence

In accordance with the directions set down in the Inquiry's Call for Evidence dated 11 December 2013, I hereby submit my own views which are those of an ordinary private citizen, aged 60, and a frequent user of telephone and email.

Executive Summary

1. My views address only the question of balance between the individual right to privacy and the collective right to security. I have no comment on the legal framework.

2. While there should be checks and balances, as in any system, this country's security services should in principle be permitted to monitor ('intercept') any and every communication system which a terrorist or other serious criminal might use in the conduct of his nefarious work.

3. Fears of George Orwell's 'Big Brother' are fanciful. It was and remains a work of fiction, and there is no risk of its becoming reality in this country.

Analysis

4. The innocent citizen. Because I have nothing to hide, I have no objection to the security services analysing my electronic communications usage (which I understand is currently the case) or – should Parliament require it in the future – reading the content of any or all of my communications in whatever form. Only if I had something to hide would I object to the authorities trying to find out what it was.

5. Nature of privacy. No-one's privacy is jeopardised unless and until the content of his communications is related to that person *as a real, identifiable person*. Until then, each of us is anonymous among the fifty (or whatever it is) million users of e-comms in this country, never mind in the rest of the world; hence the question of privacy does not at that stage arise. By way of example, if GCHQ were to pick up the content of an affectionate email from me to a woman who is not my wife, I can see no grounds for objection at that point. Someone

whom I didn't know in Cheltenham (or more likely a machine with no personal feelings) would then know that someone they don't know was sending an affectionate message to another person they didn't know. If however GCHQ identified me and told my wife, then I might object to that (assuming I was embarrassed by such disclosure) as an intrusion into my privacy. The point is that until the anonymity is removed, no-one's privacy is prejudiced. (Such misbehaviour by GCHQ would be a disciplinary matter for the individuals involved, rather than grounds for closing the place down.) It therefore follows that only if I had something to hide – something criminal, something extreme, something prejudicial to my fellow citizens – would I be concerned in case the security services read it and traced it back to me. And that is exactly what I would expect from the security services of this country.

6. The technical medium. The principle does not change: a communication is a communication, whether by carrier pigeon or the most hi-tech smartphone on G4 satellite systems, or by Twitter or Facebook. If someone is plotting with another to blow up the public, then no sensible person would tie the security service's hands behind their back by saying they can only intercept beautifully written letters in the mail but not listen to freely available wireless transmissions, emails or Twitter feeds. Indeed, if anyone – be it terrorist, head of state of a friendly nation or whatever else – is dumb enough to talk on a mobile phone over an unencrypted circuit then they must expect to be listened to, even if only by the newspapers and the Russians.

7. Metadata or content? There has been much discussion about whether what is collected is metadata or content; the former seems to be acceptable, the latter not. This is like trying to debate whether watching fairies dancing in the sunlight is acceptable: it is utterly irrelevant. If the security services actually want to listen in to an intimate but innocent telephone conversation, and then waste their time relating it to a real person, then release that information publicly so that someone is personally embarrassed, then we've got the wrong people doing the job. But I suspect the reality is that the UK and US security services are more in danger of being overwhelmed than underwhelmed by information, and in those circumstances I would do everything I could to assist – or rather, not to hinder – their search for the needle in the haystack which might just prevent my family and friends from being blown up.

8. Proportionality. When the threat to this country from terrorism is low, such monitoring only needs to be at a low level. I don't quite know what that means in practical terms, but the principle sounds good. But when the threat is higher (and I suggest that it is relatively high given the disproportionate effect on us of horrifying events such as the London bombings of July 2005, or the grotesque murder of Fusilier Rigby, both carried out by tiny groups of extremists) then we as a society should accept a higher degree of watchfulness by our security services, even were it to be intrusive (which it is not; see my point above about the nature of privacy).

9. Police state/Big Brother. There seems to be an argument that, as surveillance and monitoring of private communications are the tools of a police state, we must be at risk of becoming a police state. Examples from around the world are given of despotic regimes supported by a secret police. This is a false argument because a) the interception of communications is not on its own an indicator of a police state; and b) a secret police comes into being only as a *consequence* of the existence of a despotic regime, it is not the *cause* of it. Britain and the US are so many light years away from having a despotic regime that such fears must realistically be groundless. The 'thin end of the wedge' analysis is equally flawed: as there is no weight behind the wedge (ie there is no drive on the part of the overwhelming majority to change our political system in that direction), there is no wedge and no thin end. I might add that the disclosures by Edward Snowden display remarkable naiveté on his part, a kind of

'supermarket approach' to life where meat comes in nice clean packets and there is no death, no entrails, nothing nasty.

10. Regulation and control. It is right, however, that there should be limits to the powers of the security services, and the *custodies* themselves should be *custodiet*ed. Such surveillance and monitoring of our electronic communications must be carried out with respect to the citizen as a person, in the right frame of mind and for the specified purpose. It would be wholly unacceptable if such surveillance were to 'creep' over the years from genuine security to, for example, commercial purposes or, worst of all, controlling the dissemination of dissenting views. The parameters for the security services' operations should be set by Parliament, and those services should be answerable to and subject to the scrutiny of our democratically elected representatives at Westminster. I see no need for any more complex system in this country.

11. The IT giants. In December there was news that the giant 'IT companies themselves' were pleading for reduced surveillance/monitoring. We should be wary of indulging in inappropriate reflex reactions to their bleating. In the manner reported on the BBC news it was made to sound as though '*even they* have asked for reduced surveillance, so it must be necessary'. The giant IT companies are commercial organisations – ie, they make profit for their shareholders; they are not the guardians of either our civil liberties or our security. A quiet footnote to that news item was the IT companies' acknowledgement that if members of the public fear government surveillance/ monitoring then the public won't use their systems. This is convincing only in the context of, say, a Chinese company sending industry-confidential material by email which uses routes monitored by the security services of other countries. But that is no reason to relax our guard against material threats to our physical security. Maintaining our watchfulness may result in a slight loss of revenue to these giants, but it may also result in fewer bombs on our streets – or indeed in their own headquarters – than otherwise.

12. Effectiveness. It was asserted today on BBC Radio 4's 'Any Answers' that of all the communications intercepted by the NSA, only once had this led to the foiling of a terrorist plot. The speaker then said that, as a consequence, there is no evidence that this monitoring works. Even if the first assertion is true (as to which I cannot say), it is still no argument for not trying to do the job properly. I would not unscrew my front door from its hinges and throw it away because I 'had no evidence that it had foiled a conspiracy of burglars'. Maybe having that door there had deterred the burglars from even trying?

13. In conclusion. I do not regard myself as either paranoid or complacent about the terrorist threat. It only needs one lucky terrorist (or small group) to get through for scores of human beings to be killed or maimed because of some crackpot philosophical argument, resulting in shock and horror in hundreds of bystanders, scores or even hundreds of broken families, not to mention massive civil disruption. I cannot for the life of me see what possible objection any sane person can have to a nameless person or machine reading our emails (if they have the time) in the hope of finding the one thing that will prevent an event of bloodshed happening on our streets. This is not a game: it is a matter of life and death – possibly the life or death of our own loved ones.

Yours faithfully

Chris Todhunter