COMMENTS TO THE INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT IN RELATION TO ITS PRIVACY & SECURITY INQUIRY

1. I am Martin Hoskins and have some 25 privacy experience, providing strategic and practical approach to data protection, law enforcement, lawful interception, child safety, insurance and marketing in the financial services, on-line, telecommunications and utilities fields. From 2000 – 2012 I was employed by T-Mobile (now known as EE Ltd) as Head of Data Protection and also managed T-Mobile's Law Enforcement Liaison Department.

2. In 2012 I was appointed Specialist Advisor to the Joint Committee on the Draft Communications Data Bill. In 2012, I was also appointed to the Data Protection Advisory Panel (advising the Ministry of Justice on its approach to the EU's proposed Data Protection Regulation and Directive in the field of law enforcement).

3. I am currently an independent privacy consultant and a non-executive director of a data protection recruitment firm. I make these representations in an individual capacity.

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

4. The test of whether the correct balance has been struck between the competing rights to individual privacy or collective security will be made by people who, in the main, are influenced by a wide range of opinion formers. The balance is more of one of public opinion than it is of legal principle.

5. The Committee is likely to have received evidence from a range of privacy organisations who, for reasons of principle, are uneasy with (or are fundamentally opposed to) the concept of state surveillance. These organisations, although relatively few in number, are able to generate a very considerable amount of media comment, and appear to be able to draw public attention, almost at will, to a wide range of investigative techniques ("tradecraft") that the law enforcement community has previously tried to protect.

6. It is hard to find much evidence that there is a significant level of public concern at such tradecraft. Possibly, this is because many members of the public would expect competent law enforcement investigators to engage in such tradecraft anyway. Even though there is a relatively low level of public concern, however, it is hard to imagine that all the privacy organisations would lose faith in the legitimacy of their opposition to state surveillance.

7. The Committee is also likely to have received evidence from the "users" of private communications data, and may well have been struck by the very considerable value that such data provides to the law enforcement community. Committee members are also likely, if they have managed to visit any police force telecommunications intelligence units, to

appreciate the great care that is taken to ensure that robust safeguards are in place to prevent poor behaviour by investigators.

8. The Committee may want to ask why it is that, despite the safeguards that are evidently in place, such a wide range of privacy organisations are not reassured with these safeguards. I have seen very little evidence that the privacy organisations have been afforded much, if any, exposure to any police force telecommunications intelligence units. There appears, on the part of many stakeholders in the privacy lobby, to be a considerable lack of practical knowledge and experience of the great care that has been taken to ensure that robust safeguards are in place to prevent poor behaviour by investigators.

9. It is extremely regrettable that these privacy organisations have not been afforded better access to the law enforcement environment. If they had been more comprehensively briefed, I believe that the more pragmatically minded individuals within the privacy organisations would feel far less concerned than they do at present. From my experience of working alongside a number of senior individuals in the privacy community, law enforcement investigators will have nothing to fear from being permitted to become more transparent.

10. It is also extremely regrettable that the surveillance commissioners have not been able to satisfy the concerns of the privacy lobby. Partly this may be due to the fact that some commentators are not confident that the commissioners have sufficient resources to be seen to be doing their job adequately. But, it is also due to a failure on the part of the Government to ensure that the surveillance commissioners employ staff who are tasked with being sufficiently proactive in the public arena. The culture of the surveillance commissioners is too inwardly focussed.

How does this differ for internet communications when compared to other forms of surveillance, such as closed-circuit television cameras?

11. The regulation of public surveillance by means of CCTV technologies is fundamentally different to the surveillance of a person's private communications. CCTV surveillance invariably occurs in the public arena. Individuals generally know when they are in a public space, and are therefore capable of regulating their behaviour so that it does not cause public offence. The surveillance of an individual's communications, on the other hand, occurs everywhere and all the time. And, in my view, it has to. Even in the privacy of their own home, their soul is effectively open to public officials who need to access their digital trails for law enforcement purposes.

12. What differs, therefore, should be the access regimes for such data. It ought to be able to be easier for investigators to access CCTV data than communications data, as the consequences of the misuse of communications data are potentially much greater than the misuse of images of an individual in a public space.

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?

13. It is always necessary and proportionate to monitor and collect innocent communications when there is a certain level of pubic fear about their collective security. It is impossible, in advance, to know who may not be innocent. It is far more democratic and socially responsible to collect the communications data relating to everyone, than use screening techniques and a selection process that would inevitably discriminate between individuals. I suspect that public attitudes to surveillance in the UK, given the recent, current, and projected terrorist threat, are different to, say that of the population of Belgium and Holland, whose citizens have faced fewer recent experiences of terrorist action.

14. Given what I understand (through media reports) to be the immediate security threat, I don't see the "business case" for surveillance becoming less persuasive in the foreseeable future.

15. Having personally (but indirectly) experienced the effects of terrorist actions, I do appreciate the effect that terrorism has on the family members of the victims of terrorism. Surveillance is a relatively small price to pay if we are to live in a world where it is harder for terrorists to operate.

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.

16. The current legal framework needs to be revised to take account of the internet age. Concepts that were clearer in an analogue age, where communications records were created when telephone conversations were set up, but providers did not monitor the resulting conversation, cannot readily apply, if at all, in an on-line world today. The focus of the argument needs to move from not "what" communications data is being recorded, but "what controls" should exist to ensure that the data that emerges from these digital trails is only made available to investigators who have a pressing need to access it.

17. The focus also needs to move to that additional steps need to be taken to reassure the public that the controls are being effectively monitored by a high profile team of inspectors, and that people who abuse the information potentially available are both deterred or, if caught, appropriately punished.

18. The Committee needs to appreciate that whatever legal framework is developed, what is vitally important is that an amicable and constructive practical working relationship must exist between Home Office officials, investigators and Communication & Internet Service Providers (CSPs). The CSPs will have corporate and social obligations to protect the privacy but also safeguard the public security of their customers. But there may be cases when legal

processes potentially conflict with operational requirements. Time may be of the absolute essence. Or, there may be cases when what is presented to the provider as an operational requirement is not necessarily covered by an existing legal authority. Or, the existing authority may be set out, say, as a Direction under Section 94 of the Telecommunications Act 1984, i.e. in ways that make it difficult for a CSP to explain / justify to individuals who do not have the highest security clearances.

19. CSPs need sufficient confidence in the integrity of Home Office officials and law enforcement investigators if their operational requirements are to be met in advance of such legal authorities always providing sufficient cover.

20. Accordingly, in order to reduce the possibility of reputational damage to the CSP's brand, Home Office & law enforcement officials and surveillance commissioners have an obligation to be as transparent as they can possibly be with the public with regard to the adequacy of the safeguards that are in place to regulate what must inevitably be a deeply intrusive practice.

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

21. I commend to the Committee the recommendations of the Joint Committee on the Daft Communications Data Bill[1], which I support in their entirety.

22. Unlike other commentators, I do not feel it appropriate for individuals who have been the subject of surveillance to be informed of this fact at an appropriate time. There are a huge range of practical difficulties with this practice. For example, it could cause an innocent individual to experience considerable anguish or distress to learn that they had been subject to unnecessary surveillance, even though they had not felt (or been caused) any distress at the time of the surveillance. And, it is not at all clear whether this proposal is practical given the amount of investigative resource such a notification process would involve, nor is it clear when the notification of surveillance on one individual for one offence might compromise the prospects of successful surveillance on that individual for another (perhaps a future) offence. In my view, "let sleeping dogs lie".

17 February 2014

[1] HL Paper 79, HC 479