DRAFT EVIDENCE TO ISC

1. **In considering the balance between the individual right to privacy and the collective right to security, an excellent rule of thumb is to consider what is the greater good for the greater number of people. In my opinion, the collective right to security should always be paramount.**

2. **In the Annual Report on the National Security Strategy (NSS) and Strategic Defence and Security Review (SDSR) published in December 2013, Para 16 said "It has been a Government priority to introduce a programme to preserve the ability of the security, intelligence and law enforcement agencies to have the access they require to communications data. Communications data have played a role in 95 per cent of all serious organised crime investigations and every major Security Service counter-terrorism operation over the past decade. The Communications Capabilities Development Programme continues to provide essential capabilities under existing legislative frameworks, ensuring that the police and other public authorities have the capacity to detect, prevent, disrupt and investigate crime. As communications technologies and services continue to evolve, we need to ensure that the communications data needed by the police and others continue to be available. Changes to the existing legislative framework may be required to maintain these vital capabilities."**

3. **This illustrates the importance and necessity of the collection of communications data that is now on a vast amount of traffic because of the development of the technology of communications. The ability of the agencies has had to follow the technology. They have been forced to expand their catchment because communications technology has developed in the way it has. It is a tribute to their skill that they have managed to keep pace with this.**

4. **There is all the difference in the world between collecting information on data (A contacting B when and how) and interception (content of the communication between A and B).**

5. **Both activities are covered by legislation and the second requires a warrant under the relevant legislation. For details and a historical perspective, people can refer to the Interception of Communications Act 1985 (IOCA) and the Regulation of Investigatory Powers Act 2000 (RIPA) and to get the flavour of current thinking, the legislative changes which were proposed in the Draft Communications Data Bill which was announced in 2012 but withdrawn in 2013 after political difficulties.**

6. **As to the question of whether our current legislation is fit for purpose, I understand the Interception of Communications Commissioner, The Rt Hon Sir Anthony May is currently carrying out a study of exactly this question to report to the Prime Minister. I think such a report from such a distinguished judge with complete access to all the relevant material should provide some definitive answers. It would be useless to try to pre-empt this at this stage by others less juridically qualified and with less access.**

7. **I would like to say finally that for anyone not completely involved in this field currently and operationally, it would be impossible to know what material is or is not "damaging" by release into the public domain. One would have to know the details of what possessing the material revealed about capabilities and what this revealed to the targets who could have been unaware of their own vulnerability in using a particular method of communication. It is nonsense, therefore, for journalists and others to claim that in releasing detailed material in their possession they are not "damaging" national security when in fact they are completely ignorant of what they are revealing about capabilities of which targets could have been ignorant and even unsuspecting.**

Baroness Ramsay of Cartvale **7th February 2014**