PRIVACY AND SECURITY INQUIRY: OPENING STATEMENT

- The way we all communicate has changed dramatically in the last twenty-five years. In particular, the internet as a means of communication has had a significant impact on how we conduct our day-to-day lives.

- The extent to which communications on the internet might be accessed by others came into sharp focus in 2013 when Edward Snowden stole classified material which he then released to the media.

- This led to allegations that government agencies were engaged in blanket surveillance of the internet, and brought the debate on internet freedom into the limelight – to what extent should the internet be a private space for individuals to communicate?

- For many, the free and open nature of the internet represents liberty and democracy, and those values must be protected at all cost. For others, if the internet is an ungoverned space it is also a dangerous space, allowing those who wish to harm others to plan in secret, threatening the liberty of all.

- This tension between the individual's right to privacy and our collective right to security set the context for the Committee's Inquiry into the use of intrusive capabilities by MI5, MI6 and GCHQ.

- Over the past twelve months, we have used our strengthened powers in the Justice and Security Act to require information. We have examined several thousand pages of written evidence, received 56 substantive submissions, and held 19 oral evidence sessions, some of which were held in public.

- We have considered:
  - the range of intrusive capabilities currently available to the Agencies;
  - how those capabilities are used, and the scale of that use;
  - the extent to which the capabilities intrude on privacy; and
  - most importantly, the legal authorities and safeguards that regulate their use.

- We have today published our findings in this Report – *"Privacy and Security: A Modern and Transparent Legal Framework"*.

- The Report contains an unprecedented level of detail about the intrusive capabilities that the Agencies use – and in some cases these are capabilities that have not previously been revealed publicly – and makes 54 substantial recommendations.

- Looking first at interception, the Agencies conduct two types of interception, depending on the information they have and what they are trying to achieve...
  - First, as an investigative tool.
    - Where there is specific knowledge about a threat – for example, a specific email address has been linked to terrorist activity - then the Agencies may intercept that individual's communications, provided they can demonstrate that it is necessary and proportionate to do so.

    - This is known as 'targeted interception' and, where the target is in the UK, must be authorised by a Secretary of State under the Regulation of Investigatory Powers Act 2000 (RIPA).
    - Contributors to this Inquiry broadly accepted the principle of targeted interception.

  - Second, as a 'discovery', or intelligence-gathering, tool.
    - The Agencies can use targeted interception only after they have discovered that a threat exists.
    - They require separate capabilities in order to uncover those threats in the first place - whether those are cyber criminals, nuclear weapons proliferators or ISIL terrorists - so that they can find patterns and associations, in order to generate leads, and obtain the information they need to then target those individuals.
    - 'Bulk interception' is primarily used as a discovery tool, and it is this capability that has been at the centre of recent controversy and led to allegations that GCHQ is monitoring the communications of everyone in the UK.

- If that were the case, it would be both illegal and unacceptable. We have therefore scrutinised GCHQ's capability to intercept internet communications in very considerable detail. Our Report contains the full detail, but our key findings are as follows...

- Bulk interception involves three stages of filtering, targeting and selection. The first stage is choosing which communication links to access.
  - The internet carries the communications of around 2.4 billion internet users. In just one minute it carries 204 million emails, 4.1 million Google searches, 6.9 million Facebook messages and nearly 350,000 posts to Twitter.
  - The vast majority of these communications are carried across fibre optic cables, which carry 'bearers'. There are approximately 100,000 such bearers.
  - Of those bearers, GCHQ could theoretically access a small percentage of them.
  - However, the resources required to process the data involved mean that in practice GCHQ access only a very small percentage of what they could access. They deliberately select those bearers that are most likely to be carrying communications relating to threats to national security.
  - One of the concerns expressed to us by witnesses was that GCHQ was conducting blanket surveillance. Given the very small percentage of the bearers they access, it is clear that GCHQ do not conduct blanket surveillance.

- The second stage is selecting which communications to collect from that very small number of bearers.
  - The first major processing system we have investigated uses "specific simple selectors" to decide which items to collect. These are specific identifiers, relating to a known target.
  - Another major processing system we have examined targets an even smaller subset of the bearers GCHQ accesses. This system applies a set of "selection rules" to filter communications. This results in the majority of the communications being discarded.
  - One of the concerns expressed to us by witnesses was that GCHQ was conducting indiscriminate surveillance. However it is clear that GCHQ use filters and selection criteria to decide which communications to collect: it is not therefore indiscriminate.

- The final stage is deciding which of the collected communications to read.
  - For those communications collected under the first processing system we examined, GCHQ undertakes a “triage” process to determine which of the communications collected have the highest intelligence value, and therefore should be read.
  - Even when they know that communications relate to a known national security target, they do not have the capacity to read all of them, so they must prioritise. Only a very small proportion of those collected are ever read.
  - Another processing system runs automated and bespoke searches on the communications it has collected, combining a number of complex criteria in order to draw out those communications most likely to be of highest intelligence value.
  - To use the haystack analogy, rather than searching through the haystack of communications they have collected, they use a magnet which draws out the needles, which are the fragments of intelligence.
  - These search results are presented in list form to analysts, who rank them to decide which to open and read – they only read a very tiny percentage of those collected.

- In summary:
  - GCHQ’s bulk interception systems target a very small percentage of the bearers comprising the internet;
  - GCHQ apply selection rules and criteria so they collect only a fraction of the communications carried by these bearers;
  - GCHQ apply further targeting, searching and filtering processes to select a very tiny percentage of those communications as being those of the highest intelligence value which should be read.

- Given the extent of filtering involved, it is evident that GCHQ’s bulk interception capability does not constitute blanket surveillance or indiscriminate surveillance.

- Nevertheless, some of our witnesses considered that it is preferable to let some terrorist attacks happen rather than to allow any form of bulk interception. We do not subscribe to that point of view. We have examined cases which demonstrate that bulk interception has exposed previously unknown threats or plots which threatened our security and which would not otherwise have been detected. Therefore, in principle, we consider that bulk interception is an appropriate intelligence-gathering capability that contributes to the UK’s national security – as long as it is properly targeted and controlled.

- In examining those targeting criteria, and the controls in place, we have paid particular attention to the communications of people in the UK.
  - There is considerable confusion as to how the categories of ‘internal’ and ‘external’ communications apply to internet communications.
  - However, having scrutinised the arrangements, we have found that GCHQ can only search for and select communications to examine on the basis of a selector relating to an individual in the UK, if – and only if – they first obtain a specific authorisation from a Secretary of State which names that individual.
  - It is unlawful for them to search for and examine the communications of someone in the UK without that targeted additional authorisation.

- We have found the regulations and safeguards in place to be, on the whole, reassuring. Nevertheless, we have made a number of recommendations, primarily to address:
  - Greater transparency. For example, we have recommended the current statutory ban on ever disclosing the existence of individual warrants should be removed.

  - Strengthening the safeguards that apply to British citizens – while there are safeguards in place for people in the UK, we recommend that there should also be statutory protections for British Citizens overseas.
  - And we have recommended improved safeguards around sensitive professions, such as lawyers or doctors or journalists.

- Moving on from bulk interception, we also heard concerns expressed over the Agencies' use of Communications Data – the 'who, when, and where' of a communication.

- This debate is complicated by widespread confusion as to what information is CD, and what is content. We consider that there is in fact a 'grey' area between the two. For example, web domains visited or the locational tracking information in a smartphone.

- This information, while not content, nevertheless has the potential to reveal a great deal about a person's private life. We have therefore recommended that it should be treated as a separate category which we have called 'Communications Data Plus'. This should have greater safeguards than the narrowly drawn category of Communications Data.

- In terms of the other intrusive capabilities used by the Agencies, our Report contains a number of detailed recommendations, primarily in relation to specific statutory oversight and greater transparency - where that is possible without damaging national security.

- We have sought throughout this Report to publish as much information as possible, as we consider it essential that there is greater transparency. Crucially, our Report reveals for the first time the Agencies' use of Bulk Personal Datasets. This has not been publicly acknowledged before this morning, and we recognise the work of the Intelligence Services Commissioner in achieving this.
  - Bulk Personal Datasets are large databases containing personal information about a wide range of people. The Agencies use them to identify individuals during the course of their investigations, to establish links between Subjects of Interest, and to verify information that they have gathered through other means.
  - We have seen all the datasets that the Agencies hold and are satisfied that they are held for a lawful purpose, and are necessary and proportionate.
  - Avowal is an important first step, but we recommend that the Government consider what further information can be placed in the public domain, and recommend that the oversight arrangements be placed on a firm statutory footing.
  - The same is true of the Agencies' use of the Telecommunications Act, which we have also avowed for the first time in our Report.

- However the most significant finding in our Report relates to the legislative framework that governs the use of all these intrusive capabilities. At present, there is no one piece of legislation that governs what the intelligence and security Agencies can and cannot do. The current framework is unnecessarily complicated.

- While we have seen no evidence that the Agencies are seeking to circumvent the law - in fact, the care and attention given to complying with the law within the Agencies is highly commendable - the lack of clarity in the existing legislation has fuelled suspicion.

- However, minor reforms and improvements around the edges of the existing legislation are not sufficient in the long term. Therefore, rather than simply reforming RIPA, as some have suggested, we consider that the entire legal framework, as it applies to the intelligence Agencies, needs replacing.

- The purposes, functions, capabilities and obligations of the Agencies should be clearly set out in a new single Act of Parliament. This should also include the privacy constraints, transparency requirements, targeting criteria, sharing arrangements and other safeguards that apply to the use of their capabilities.

- These changes are overdue. There is a legitimate public expectation of openness and transparency in today's society. Therefore, while the Agencies must operate in secret if they are to be able to protect us – and we cannot expect them to do their job otherwise - every effort must be made to ensure that information is placed in the public domain when it is safe to do so.

- Our Agencies do a very important, and difficult job, in difficult times. We believe that the public should have every confidence in them, and we believe that greater transparency about their work will improve public understanding and reinforce that confidence. We hope the Report that we are publishing today will contribute to that confidence.

[ENDS]