JOINT COMMITTEE ON THE DRAFT INVESTIGATORY POWERS BILL

LAW ENFORCEMENT – WRITTEN EVIDENCE

Overarching/Thematic Questions:

1. **Are the powers sought necessary? Has the case been made, both for the new powers and for the restated and clarified existing powers? Are the powers sought legal? Are the powers compatible with the Human Rights Act and the ECHR? Is the requirement that they be exercised only when necessary and proportionate fully addressed?**

    a. Law Enforcement (LE) believe that the powers are absolutely necessary as a part of the overall mix of capabilities they require for protecting the public. The powers considered in the draft Investigatory Powers Bill (IPB) streamline and update the legislation in the areas of Communications Data (CD), Lawful Interception (LI) and Equipment Interference (EI), ensuring that they address privacy concerns and provide a more transparent regime with rigorous oversight. The powers are all vital tools required to bridge the gap that is developing between criminal use of technology and LE's ability to operate effectively in this dynamic digital environment. Additional detail on the changing technological landscape is provided in **Annex A**.

    b. LE do not consider that the IPB introduces any 'new' powers. Instead it enables existing capabilities to be maintained in the digital environment. The LE requirement for CD has been consistent for many years; the crime types that are investigated have changed little though technology has enabled criminals to develop old crimes in new ways, and made certain types of crime more accessible; the technology that supports those that wish the public harm has changed, and now includes the rise of cyber-enabled and cyber crime. The only change introduced in the IPB is the requirement for Communication Service Providers (CSPs) to retain more information on their customers' use of their services (Internet Connection Records (ICR)) and provides a statutory footing for LE to request this data under specific, targeted circumstances. Additional detail on what an ICR might look like is provided in **Annex B**.

    c. LE act in accordance with the law and existing processes already ensure that the activities which are the subject of the IPB always consider the

implications and impact of the Human Rights Act[1] and the ECHR whatever activity they are considering and whatever power that they might use. On every occasion, necessity, proportionality and collateral intrusion, where it might occur, are considered during each stage of the application and authorisation process.

d. It should be remembered that LE work is evidential, which is different in many respects from the Security and Intelligence Agencies (SIAs), and it is targeted. Unlike the SIAs our work is often subject to the test of scrutiny in a court and is subject to external, rigorous oversight and disclosure. The capabilities LE use are brought to protect the public but also to bring people to justice and to discount people and prove alibis.

2. Are the powers sought workable and carefully defined?

a. LE believe they are; there remain areas where LE expect clarification to be provided on how the powers will work in practice but believe a practical and technical solution could be implemented in order to deliver the capabilities LE need.

General Questions:

3. Are there any additional investigatory powers that security and intelligence services or law enforcement agencies should have which are not included in the draft Bill?

a. LE identified five core operational requirements for CD which were articulated during the review of powers by David Anderson QC, and set out in his report 'A Question of Trust'. These are to:

- **i.** Link an individual to an account or an action
- **ii.** Establish a person's whereabouts
- **iii.** Establish how suspects or victims are communicating
- **iv.** Observe online criminality, and
- **v.** Exploit data [to corroborate evidence, identify further investigative leads]

b. These remain LE requirements for investigations. Under current legislative provisions, particularly for CD, LE is increasingly unable to meet these five requirements when a suspect or victim's activity takes place online. The IPB goes a long way to meeting these requirements, but a restriction has been

[1] For example, LE often has to balance a matrix of qualified rights such as privacy and freedom of thought, expression, and non-discrimination with that to save life and protection of persons and fair investigation and trial.

placed in the IPB in respect of exploitation of ICRs that will significantly reduce investigative capabilities.

c. S.47 imposes restrictions on the granting of authorisations, limiting the purpose for which ICRs can be obtained to identifying - who has used an internet service, where the service and time of use are known (Internet Protocol Address Resolution (IPAR)); which Communications Services a known individual has used and where or when a known person has accessed illegal material. These provisions significantly restrict the opportunities that an investigator may develop from the information derived from ICR's and mean that not all five LE requirements can be met. There are a number of examples in **Annex D** that draw this point out.

d. In essence, and in both proactive and reactive investigations, if LE are denied the opportunity to derive information from ICRs that are not those set out in s.47, for example information pertaining to such activities as using a travel webpage, a banking service, a car rental company, or making online purchases, then investigative opportunities are unknown and investigations may cease altogether. This is because it will be very rare for any other opportunities to exist. This pursuit of different lines of enquiry is normal tradecraft for most investigators, whether it be for a missing person or the understanding of conspiracy by an organised crime gang. This problem does not/did not occur where traditional telephony is used and call records indicate that a voice call took place but with the advent of voice being made into data travelling from one IP address to another, then ICRs are vital for LE to retain the capability to pursue enquiry opportunities.

e. If it is assumed that ICRs are to provide LE with avenues for investigation, where those avenues cannot be explored due to jurisdictional limitations, the IPB makes no provision for alternative approaches (for example under Mutual Legal Assistance). This is particularly relevant to overseas service providers in jurisdictions where UK LE have no legal recourse and where it is unlikely there might be any formal or informal cooperation. This issue may have been addressed under the third party provisions, but there is no requirement placed in the IPB for the retention of third party data that does not originate or terminate on a UK CSP's network.

f. In a separate issue, s.46 sets out the purposes in which a designated senior officer may authorise access to CD. These are comprehensive but LE is concerned in respect of the wording in s.46 (7) (g) which allows for CD to be obtained, where necessary and proportionate, for the purpose of preventing death, injury or damage to a person's physical or mental health – in an emergency. It is within this 'emergency' category where there may be potential difficulties. Hundreds of people are reported as missing in the UK every year, many of them are classed as vulnerable due to their age or mental or physical health and LE would rightly seek to limit the danger to which such individuals are exposed by locating them as soon as reasonably practicable. Not all instances would be deemed an 'emergency' and it is unclear why CD cannot be used as a tool of early consideration rather than meeting the requirements of last resort to prevent harm to an individual. LE believes that 'saving life' should be explicitly available as a justification to

avoid emergency situations. LE believe that the term 'emergency' should be referenced as being for civil contingencies such as kinetic transport disasters; rail or air crashes or terrorist incidents where the identification of people for emergency response will be required by LE as the lead for public authorities.

g. Finally, the practical implementation of the provisions of the IPB, by LE and by industry, may take time to be fully effective, and so there will remain gaps in LE investigative capabilities until full implementation is achieved.

4. Are the new offences proposed in the draft Bill necessary? Are the suggested punishments appropriate?

a. LE do not believe it is necessary to introduce additional offences above those that already exist in legislation or in common law (for example Misconduct in Public Office) which already cover the proposed offences outlined in the Draft Bill.

b. In particular, the concept of 'reckless' proposed in the Draft Bill, whether this may be clarified in any Code of Practice, does not make it clear what the offence is attempting to cover when no offence is committed if the CD is obtained under an authorisation.

c. Subject to the requirements of Parliament, should such an offence be deemed necessary, then 'reckless' could be more appropriately replaced so that an offence is only committed when a person intends to acquire CD without an authorisation. This is consistent with the offence in s.2 which provides that an offence is committed if there is intentional (not reckless) interception.

Interception Questions:

5. Are there sufficient operational justifications for undertaking (a) targeted and (b) bulk interception?

a. The IPB does not permit LE to conduct 'bulk' interception. All LE lawful interception (LI) is tightly targeted and provides LE with significant operational benefits. It is used as a source of intelligence which assists in identifying and disrupting threats from terrorism and serious crime. It supports the gathering of evidence and identification of opportunities, where it meets the necessity and proportionality thresholds, eg. to tackle the supply of prohibited drugs, people trafficking, fraud, child sexual exploitation, firearms and the proceeds of crime. The importance and dependence on the intelligence provided through targeted LI is likely to remain of vital importance.

b. In the broader LE context, but very specific to how targeted LI is used by HMRC, the following illustrates how important such capability is:

   i. HMRC faces a number of key organised crime threats including cigarette and tobacco smuggling; alcohol smuggling and diversion; the smuggling and laundering of oils; VAT multi trader intra

community (MTIC) fraud; and non MTIC attacks on HMRC repayment systems including Self-Assessment, VAT and Gift Aid.

ii. Targeted interception is a key capability which provides HMRC with the intelligence to support operational activity which leads directly to arrests, seizures (of contraband, criminal assets and money) and prosecutions. But it also makes a significant contribution to HMRC's strategies to counter organised attacks on its systems. Interception can provide a clear understanding of criminal techniques and strategies. This intelligence is used to drive changes in policy, processes and legislation to strengthen any weaknesses in HMRC's systems that crime groups may seek to exploit. Interception is an agile tool that can keep pace with the speed with which crime groups adapt to changes in HMRC's control methods. In 2014/15 targeted interception and communications data supported investigations that prevented just over £2 billion in revenue loss.

6. Are the proposed authorisation processes for such interception activities appropriate? Is the proposed process for authorising urgent warrants workable?

a. LE consider that the proposed authorisation for a 'double lock' process, where it provides additional oversight and transparency by a Judicial Commissioner can be supported, subject to there being no impact on the current regime of flexibility and agility of response in a dynamic 24/7 environment.

b. LE is concerned that the urgent out of hours authorisation process for modifications to a Warrant has been adversely impacted by the proposed increase in grade/rank for such authorisations. The limited availability of such senior officers risks creating delays in operations given that they also have limited time available to make authorisations. This could, perversely, lead to a reduction in safeguards with senior officers taking less time to examine applications. LE would seek to use the current process whereby a suitably trained, experienced and accredited Superintendent may authorise a modification in such circumstances.

Communications Data Questions:

7. How well does the current process under Mutual Legal Assistance Treaties (MLATs) work for the acquisition of communications data? What will be the effect of the extra-territorial application of the provisions on communications data in the draft Bill?

a. Mutual Legal Assistance is the formal way in which countries request and provide assistance in obtaining evidence located in one country to assist in criminal investigation or proceedings in another country. Mutual Assistance in Criminal Matters between the Member States of the European Union supports the exchange of information and includes a section on requests for communications data that are routed through the relevant Central Authority. In light of the significant proportion of communications providers based in

the United States of America, there is a Mutual Legal Assistance Treaty between the UK and the USA.

b. The process for LE acquisition for CD through the MLAT process, involves meeting the administrative and judicial standards for evidence (or relevant request) in the requesting country, passing the request to a Central Authority that checks the request for compliance with national MLA legislation and the relevant treaties, and then passes this to the receiving country's Central Authority, who also check for compliance with their national MLA, relevant treaties and the national legislation governing the request. The receiving Central Authority will then pass it to a national authority who can turn the international request into a national request under the receiving country's legislation and national administrative processes. This may include, as it can in the USA, making a request to a court for a relevant warrant or order and then this being passed to law enforcement to serve on a company. Unless any of the individuals' or authorities' sole focus is on international cooperation - like the Central Authority, or some specialist departments in US District Attorney's Offices - carrying out the administrative process for a foreign country is likely to be a task added onto their normal workload. In addition to this, the request is likely to be written to fulfill the requesting country's administrative and legal practices, not in those of the receiving country's. This includes omitting specialist language that particular requests may require.

c. The current process may take several weeks, or even months and there is therefore no guarantee that requests will meet with deadlines for trial. Work is underway however to streamline the processes, including moving several of the stages from 'hard copy' on to an electronic system. Despite these improvements, Mutual Legal Assistance is not a substitute for obtaining data under the IPB as, given the inevitable time-constraints in the process, MLAT does not support agile intelligence development during a criminal investigation. All reasonable steps have been taken to improve the process over the past two years, including comprehensive training and awareness programmes initiated to enhance awareness of investigators and prosecutors for the early identification of MLAT opportunities. Whilst the quality of the data returned will continue to meet LE requirements, this streamlining will significantly improve how well the current process functions. LE recognises the efforts in this area but would welcome any further legal provisions which could assist in achieving faster and more agile responses.

d. UK law is clear that companies providing communications services to users in the UK, irrespective of where they are based in the world, must comply with lawful requests from the UK authorities. The UK Government intends to maintain these obligations in the IPB. We expect any multinational firms operating in any industry in the UK to act in accordance with our laws and we have always sought to work with companies to this end.

8. Does the draft Bill allow the appropriate organisations, and people within those organisations, access to communications data?

a. Please see our response to Q3 above.

b. CD is regularly used as evidence in criminal prosecutions. Largely, the data entering the criminal justice system comes from data retained under legislation. CD provides vital evidence of:

- **i.** Chronology (the time and sequence of events in relation to a particular case – CD is more reliable than witness memory of events, for example);
- **ii.** Association (victim with witnesses or suspects, suspects with one another);
- **iii.** Presence or otherwise in a geographical locus (not necessarily at a particular location – can also be vital, in certain circumstances, from a defendant's perspective);
- **iv.** Corroboration (of other evidence in the case and in particular of the testimony of criminal or vulnerable witnesses).

9. Is the authorisation process for accessing communications data appropriate?

a. LE believe that the current process is appropriate: It is explained in diagrammatic form at **Annex C**, and was commended in the Report of the Draft Communications Data Bill (2013) and by European Commissioners during their review of the Data Retention Directive (2014).

10. Is accessing Internet Connection Records essential for the purposes of IP resolution and identifying of persons of interest? Are there alternative mechanisms? Are the proposed safeguards on accessing Internet Connection Records data appropriate?

a. The information provided below is in addition to the explanation above and that contained in the ICR annex.

b. IP addresses are a fundamental requirement to enable devices to communicate over the internet. Due to a shortage of IP addresses, however, CSPs have to share single IP addresses across several thousand users in any one instant. There is often a requirement, as part of an investigation, to identify who was accessing a service from a known IP address at a particular time. The challenge of mapping use of a single IP address back to a single user is further exacerbated due to discrepancies between server times across the world. This results in law enforcement having to allow a margin of error, in terms of seconds or minutes, when seeking resolution.

c. Given that in any one instant there may be several thousand users on the same IP address the inclusion of the relevant port number, even were it available in most investigations, (which it is not), – does not sufficiently refine the search to enable accurate resolution. In the time window LE may have to provide there may be several people allocated the same IP address and same port number.

d. If LE could structure their query in terms of- who was using this IP address (and this port number if available) and using this specified service, the resultant response would be as refined as is technically possible, thereby

reducing collateral intrusion to an absolute minimum. LE will frequently know the relevant service, whether it is an event conducted through for example. Hotmail, Facebook or Twitter, and could provide this as part of the query. Previously there was little point in providing this additional detail because CSPs had no way of tailoring the query of their system to this level. In order to do so they would require collection of ICRs.

e. The Counter Terrorism and Security Act 2015 (CTSA) provisions were intended to provide LE with the ability to resolve an IP address to an individual through the resolution of an IP address to a person or device. The provisions under CTSA did not however, permit the destination IP address or service name to be stored, therefore IP Address Resolution (IPAR) would not resolve to an individual in the majority of cases. Following Royal Assent for CTSA, LE has worked with the Home Office to determine how IPAR could be implemented and to determine what data would be required to be retained by the UK CSP. We established that in order to resolve an IP address to an individual, specific data needs to be retained which goes further than that specified in CTSA. The additional data required to be stored is the source IP address, the source port number, the destination IP address (or service name). It is this record, coupled with data and time information, that allows the reduction of the number of individuals to which the information will resolve to. This is why full ICR retention is imperative to the ability to enable IP address resolution for retrospective investigations.

Equipment Interference Questions:

11. Should the security and intelligence services have access to powers to undertake (a) targeted and (b) bulk equipment interference? Should law enforcement also have access to such powers?

a. The IPB provides the ability for LE to authorise and undertake targeted equipment interference (EI). LE will not have access to bulk EI powers.

b. EI is currently authorised and conducted by LE under the Police Act 1997 (together with other authorisations as appropriate, including RIPA surveillance authorisations). The IPB consolidates this existing legislation and sets out a clear framework for the authorisation of equipment interference.

c. LE currently use a variety of EI techniques to prevent and detect serious crime. These different techniques range in sensitivity, complexity and intrusiveness and are deployed in a targeted and proportionate way. At the more intrusive end of the spectrum EI could be used by LE as part of a proactive investigation, for example to retrieve data from a criminal's electronic device for use in evidence. At the less intrusive end, EI could be used by LE to acquire specific data for intelligence only purposes (such as to identify the methods of communication used by an organised crime group to conduct their criminal activities). Equally, EI is a crucial tool in responding to emergency situations, such as a kidnap, where the ability to quickly use these techniques can be the difference between life and death.

d. EI already provides significant operational benefit to LE by facilitating the obtaining of information and evidence that can not be captured by other

means – for example where encryption technology is being used to hide criminal communications. However, as technology develops and criminals become ever more sophisticated with it, EI will become an increasingly crucial tool for LE in maintaining its ability to effectively prevent and detect serious crime.

e. LE also considers EI techniques to be essential for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health. The IPB currently makes no provision for authorising EI for this purpose, and LE consider it should be included.

f. It is understood that the Home Office intends to limit, in the Codes of Practice, access to the more advanced and intrusive techniques to specialist units within LE. This approach will assist in ensuring that EI techniques are deployed proportionately and by those with relevant expertise.

12. Are the authorisation processes for such equipment interference activities appropriate?

a. The authorisation process requires all EI warrants be issued by a law enforcement chief and approved by a Judicial Commissioner. This will ensure detailed scrutiny and independent consideration of all EI warrants.

13. Are the safeguards for such activities sufficient?

a. LE recognise the responsibilities and obligations placed upon it by the safeguards provided for in the IPB and agree that these are necessary to protect the interests of those whose data is obtained under an EI warrant.
b. Accordingly, LE will put in place arrangements for ensuring material obtained under an EI warrant is held securely and handled appropriately. Importantly, the safeguards recognise that material obtained under an EI warrant can be used in evidence and, in appropriate circumstances, it will be necessary to disclose this material. Accordingly, the provisions provide for arrangements to be put in place that take into account the use of material in legal proceedings and the performance of the functions of LE agencies.
c. LE also recognises the importance of preserving the evidential integrity of equipment that has been the subject of EI. This will continue under the IPB and LE will work closely with prosecutors to ensure the fairness of any prosecution.

Additional Matters:

14. Retention Periods

a. Considerable detail was captured during an ACPO Data Communications Group evidence capture exercise during a two week period in 2012. The data and evidence from that report is provided at **Annex E**.

b. In a recent Child Sexual Exploitation (CSE) major operation, where Communications Data played almost the sole route for supporting the

investigation, the NCA was able to deal with 92% of the requests for CD. The remaining 8% were already more than 12 months old and for which no data would have been retained. If reduced periods were imposed on this particular operation, then it would have had the following effect:

i. Period reduced to 9 months – 66% potentially resolvable
ii. Period reduced to 6 months – 39% potentially resolvable
iii. Period reduced to 3 months – 13% potentially resolvable.

c. So if retention periods are reduced, and particularly for this crime type, it is unlikely that the NCA could have carried out such an operation, with the commensurate loss of opportunities to identify serious offenders and protect or safeguard children at risk of or suffering abuse.

15. Protective Security

a. Law Enforcement rely on a number of Government mandated standards for managing protective security. They are designed to be implemented to mitigate identified and assessed risks. The baseline for protective security is founded upon:

i. Personnel Security: Due diligence followed by an enhanced national security vetting is conducted to ensure that law enforcement officers and staff maintain a level of integrity, honesty and trustworthiness that is commensurate with the information they can access. These processes are additionally supported by a comprehensive vetting aftercare process, to manage changes in circumstances and risks.
ii. Physical Security: Both physical and procedural security measures are deployed, such as robust building design, locks, alarms and auditable access control systems to protect law enforcement activity and data from unauthorised access.
iii. Information Security: Confidentiality, Integrity and Availability of data is assessed and proportionate protection, auditable access control, and secure data storage are implemented to prevent unauthorised access. This is additionally enhanced with a proportionately robust audit process.
iv. Training: All officers and staff that are involved in the processing of applications for investigative powers undergo mandated training relevant for the role; for example the Single Points of Contact (staff with responsibility for acquiring the data from a CSP) undergo formal and continual assessment before they can be issued with a "Personal Identification Number" that grants them access to a CSP's data.

Annexes:

A. Technology and the Impact on Investigations (Q1).
B. IPB Provisions for CD (Internet Connection Records) (Q1).
C. Authorisation Process for Accessing CD (Q9).
D. Threat Picture Operational Examples (Impact of the CD clauses of the IPB) (Q3).

E. 2012 SPOC Survey (Q14).