UK RESPONSE TO COUNCIL OF EUROPE HUMAN RIGHTS COMMISSIONER – MEMORANDUM ON SURVEILLANCE AND OVERSIGHT MECHANISMS IN THE UNITED KINGDOM

Any review of investigatory powers must begin with an understanding of the context in which they are used. The powers available to the United Kingdom Government remain critical to the protection of national security, notably against the threat from terrorism. Recent events across Europe have emphasised the nature of that threat and its devastating consequences. Under the European Convention on Human Rights, it is properly for States to judge what systems are necessary for the protection of the general community from such threats, subject to supervision by the Strasbourg Court. There are significant privacy interests in play. They must however be weighed against the need for the State to protect itself and its citizens. It is important that, in assessing the detail of appropriate protection, care is taken not to risk undermining the proper effectiveness of the systems for obtaining life-saving information and intelligence that cannot be obtained in any other way.

Terrorists and criminals are communicating in ever more sophisticated ways. Ways that avoid detection, whether that be through the use of encryption, the adoption of bespoke communications systems, or simply the volume of internet traffic in which they can now hide their communications. The internet is now used widely both to recruit terrorists, and to direct terrorist attacks, as well as by cyber criminals. It is essential that the safeguards built into the United Kingdom's domestic regime continue to meet the standards established through Strasbourg jurisprudence, as described above, without damaging the ability to safeguard national security and combat serious crime, particularly at a point where advances in communications technology have increased the threat from terrorists and criminals using the internet.

The UK Government recognises the need to ensure as much transparency as possible surrounding these powers, whilst maintaining a level of secrecy about the details which is necessary if they are to remain effective. That is why the Government has introduced the Investigatory Powers Bill.

The Investigatory Powers Bill will govern the use and oversight of investigatory powers by the law enforcement and security and intelligence agencies and by other specified public authorities.

It builds on the work of three comprehensive reviews undertaken in the last two years. Those reviews, carried out by David Anderson QC, the Independent Reviewer of Terrorism Legislation, the Intelligence and Security Committee of Parliament (ISC), and a panel convened by the Royal United Services Institute (RUSI), between them made 198 recommendations.

All three reviews agreed that the use of these powers will remain vital to the work of the law enforcement and security and intelligence agencies in the future. Collectively, they proposed reforms to the way these powers are overseen and recommended the introduction of stronger safeguards and greater openness.

In November 2015 the Government published a draft Bill for pre-legislative scrutiny. The provisions in the draft Bill were considered by the House of Commons Science and Technology Committee, the Intelligence and Security Committee of Parliament and by a Joint Committee of both Houses of Parliament convened to scrutinise the draft Bill.

Between them, those Committees received around 200 submissions and held a number of evidence sessions with the Government, industry, civil liberties groups and other bodies. In response to their

recommendations, the Government introduced a revised Bill to Parliament on 1 March, alongside further explanatory material.

The Investigatory Powers Bill will transform the law relating to the use and oversight of these powers. It will strengthen safeguards and introduce world-leading oversight arrangements. The Bill will do three things:

- First, it will bring together powers already available to law enforcement and the security and intelligence agencies to obtain communications and data about communications. It will ensure that these powers – and the safeguards that apply to them – are clear and understandable.

- Second, the Bill will radically overhaul the way these powers are authorised and overseen. It will introduce a 'double-lock' for interception warrants, so that these – and other warrants – cannot be issued by the Secretary of State until they have been approved by a judge. And it will create a powerful new Investigatory Powers Commissioner (IPC) to oversee how these powers are used.

- Third, it will make sure powers are fit for the digital age. The Bill will make provision for the retention of internet connection records (ICRs) in order for law enforcement to identify the communications service to which a device has connected. This will restore capabilities that have been lost as a result of changes in the way people communicate.

The Investigatory Powers Bill will protect both privacy and security. The Bill and the accompanying draft Codes of Practice make clear the strong privacy safeguards that apply to all of the powers in the Bill, in particular:

a. Transparency: the Bill makes more explicit the powers available to public authorities to obtain communications or communications data. In doing so, it puts on a clearer statutory footing some of the most sensitive powers and capabilities available to the security and intelligence agencies. Some powers will remain outside of the Bill. For example, in line with the recommendation made by David Anderson QC, the police will retain the ability to use overt search and seizure powers to obtain communications that have been stored on a device or a server, such as emails stored on a web-based server. The Bill also imposes requirements on the Investigatory Powers Commissioner to report to the public and to Parliament precisely how the powers in the Bill have been exercised.

b. Authorisation: The Bill overhauls the way the most sensitive powers available to law enforcement and the security and intelligence agencies are authorised. Under the Bill, warrants will be subject to a new 'double lock', so that they must be approved by a Judicial Commissioner before they can be issued by the Secretary of State. This will preserve democratic accountability and introduce a new element of judicial independence into the authorisation process. This powerful new safeguard was endorsed by the Joint Committee convened to scrutinise the draft Bill.

c. Oversight: The Bill creates a world-leading oversight regime, bringing together three existing commissioners and providing new powers and resources to an independent Investigatory Powers Commissioner (IPC). The Commissioner will hold, or have held, high judicial office and will oversee the use of the powers in the Bill by public authorities. The Bill strengthens

the office of the IPC further. Where the IPC in the course of his or her investigations determines that a person has been the subject of a serious error, the IPC will have the ability to notify the individual concerned.

d. Limited powers: the Bill strictly limits the circumstances in which the powers it provides for can be used. In line with the recommendation made by the Intelligence and Security Committee in its 2015 Privacy and Security report, the Bill and the accompanying Codes of Practice make clear:

    i. The purposes for which each of the powers in the Bill may be used;
    ii. The overarching human rights obligations which constrain the use of the powers in the Bill;
    iii. Whether each of the powers in the Bill must be used in a targeted way or provides for the acquisition of data in bulk;
    iv. The authorisation procedures that must be followed, including the review, inspection and oversight regime;
    v. Specific safeguards for certain sensitive professions or categories of information;
    vi. Safeguards and obligations in respect of retention, storage and destruction of data;
    vii. Safeguards relating to sharing of material obtained under the powers in the Bill.

e. Penalties for misuse: the Bill sits alongside existing legislation such as the Computer Misuse Act 1990 to make clear the circumstances in which it is an offence to obtain communications or communications data without a lawful authorisation.

This note responds to the recommendations made by the Council of Europe Human Rights Commissioner in their memorandum on surveillance and oversight mechanisms in the United Kingdom.

Recommendation:

A range of surveillance oversight mechanisms exist in the UK which ensure that public authorities act in ways that are compatible with the Human Rights Act 1998. As far as independent oversight institutions are concerned there exist three relevant Commissioners: the Interception of Communications Commissioner, the Surveillance Commissioner and the Intelligence Services Commissioner. As for parliamentary oversight, the Intelligence and Security Committee ("ISC") provides oversight of the use of investigatory powers by the security and intelligence services. As for a judicial body, the Investigatory Powers Tribunal ("IPT") hears complaints about conduct in connection with the interception of communications and gathering of communications data by all authorities.

Dominic Grieve QC has headed the ISC since September 2015. The ISC was first established by the Intelligence Services Act 1994 to examine the policy, administration and expenditure of MI5, the Security Service, and MI6, the Secret Intelligence Service, and the Government Communications Headquarters ("GCHQ"). The Justice and Security Act 2013 reformed the ISC making it a Committee of Parliament, providing greater powers and increasing its remit (including oversight of operational activity and the wider intelligence and security activities of government). Other than the three intelligence and security Agencies, the ISC examines the intelligence-related work of the Cabinet Office including the Joint Intelligence Committee, the Assessment Staff and the National Security Secretariat. The Committee also provides oversight of the Defence Intelligence in the Ministry of Defence and the Office for Security and Counter-Terrorism in the Home Office.

The Commissioner was struck by the fact that this important Committee only has six permanent staff members. Oversight committees, such as the ISC, need to have sufficient resources, technical expertise and legal means, as well as access to relevant documents. The Commissioner calls for adequate financial and human resources to be given to the ISC. This is in line with recommendation 19 of the 2015 Issue Paper on Democratic Oversight which underlines the importance of oversight institutions having the necessary human and financial resources to fulfil their mandates.

Surveillance experts highlighted a structural problem with the make-up of the Committee where the Prime Minister has a veto on the Committee's membership and on its reports. Indeed, the Prime Minister may redact any matters he considers should not be published. The Commissioner is concerned that the executive control of this Committee may be too strong, although the new ability of the ISC to elect its own Chair is potentially significant, and the ISC's critical report of the IP Bill in February 2016 demonstrates its independence. Nevertheless, and in line with recommendation 13 of the 2015 Issue Paper on Democratic Oversight, the Commissioner recommends that the members of the ISC are appointed by Parliament as is the case with other Parliamentary Select Committees and that the Committee has the final say on what is published.

Response:

The ISC are allocated a budget of £1.3 million a year, enabling a permanent staff of 13 to support the Committee. Resources are an area that is and must be under constant review, but the ISC's comprehensive report on Privacy and Security was as detailed, technically informed and comprehensive as any such report published globally; it would be wrong to characterise this as an area of weakness in the UK system.

Members of the ISC's staff work with the Agencies and the Departments to obtain information on the ISC's behalf, ensuring that the ISC has all the information it needs to do its job in relation to matters consistent with its remit. This includes regular access to protectively marked information that is sensitive for national security reasons. The ISC members are appointed by Parliament, by vote on a motion of the relevant House. The Prime Minister can only redact material considered to be prejudicial to the continued discharge of the functions of the Intelligence Agencies or of the wider intelligence and security community. Any ISC report that has had material redacted from it will contain a statement to that effect. The Government works constructively with the ISC to ensure that as much of its reports that can be published, is published.

Recommendation:

The IPT was established in October 2000 under section 65(1) RIPA. The IPT hears allegations of wrongful interference with communications as a result of conduct covered by RIPA. The Tribunal provides a right of redress for anyone who believes they have been a victim of unlawful action under RIPA or wider human rights infringements. It has extremely broad standing requirements which enable it to proceed on the basis of assumed facts, which the government may refuse to confirm or deny.

The number of cases judged by the Tribunal to be 'frivolous or vexatious' has remained high since it began its work in late 2000. Up until 2013, the IPT had only upheld 10 complaints out of the 1,673 it had received and none of them against the security and intelligence agencies.6 As for the 2015 statistics: 47% of complaints were ruled as 'frivolous or vexatious' and 30% received a 'no determination' outcome; another 17% were ruled out of jurisdiction, withdrawn or not valid; and 3% were ruled out of time.

However, in 2015 the IPT delivered three judgments identifying a breach of rights of the European Convention on Human Rights ("ECHR"). The Commissioner shares the view of the surveillance experts that these cases show the importance of notification of surveillance. Notification is a requirement that persons who have been subjected to surveillance are notified after the fact, and subject to standard caveats, for example, only if notification would not prejudice ongoing operations. Without the revelations of Edward Snowden as to the activities of the UK surveillance services, it is unlikely that these complaints would ever have been brought.

According to the rules of the Tribunal, proceedings, including any oral hearings, shall be conducted in private, although in certain cases open hearings can and do take place. The Commissioner heard complaints from the surveillance experts, some of whom had brought litigation to the IPT, that the proceedings were opaque and secret. He therefore welcomes the fact that in 2015 the Tribunal sat on 15 occasions in open court, relating to 20 complaints.

Another issue which was raised by the surveillance experts was the "Neither Confirm Nor Deny" (NCND) policy of government. According to this policy the government neither confirm nor deny whether they are monitoring the activities of a particular group or individual, or have had contact with a particular individual. Similarly, the long-standing policy of the UK government is to neither confirm nor deny the truth of claims about the operational activities of the Intelligence Services, including their intelligence-gathering capabilities and techniques. Accordingly, it is not within the remit of the Tribunal to confirm or deny whether or not a warrant or authorisation has been issued against a member of the public, unless it is subsequently found to be unlawful. The Commissioner finds the "NCND" policy problematic in that it prevents a person from ever knowing if he/she has been the target of surveillance. Improvements to notification requirements could help alleviate this problem. At the same time, NCND shields surveillance decisions from effective scrutiny. The Commissioner welcomes the recent efforts of the IPT towards increased transparency of its procedures and encourages it to make further efforts towards this goal.

There is currently no avenue of appeal in respect of decisions taken by the Tribunal. The Commissioner welcomes the fact that the IP Bill will now include a domestic route of appeal from the Tribunal on a point of law against a final determination, although this does not provide for appeal in respect of interim legal findings during the conduct of the proceedings. The Commissioner supports

the recommendation made for changes to enable the IPT to make declarations of incompatibility pursuant to Section 4 of the HRA 1998, which would improve effective access to justice.

The Commissioner recommends increasing the transparency of the proceedings, which promote public knowledge and confidence in the oversight procedures. This should include increasing the adversarial testing of relevant evidence by way of the appointment of a Special Advocate. This would contribute to increasing the credibility of the IPT as an effective oversight mechanism. According to the Anderson report a security-cleared counsel to the tribunal may actually be more influential.

Response:

The Investigatory Powers Tribunal (IPT) plays a crucial and effective role in the UK's system of oversight mechanisms, as was acknowledged by the European Court of Human Rights in the case of *Kennedy v UK* (26839/05).

While a high proportion of cases are deemed frivolous or vexatious (the former referring to unsustainable cases, the latter often to repeated claims), this determination is always made by at least two members of the Tribunal. In cases where the IPT has found in favour of the claimant, it has provided appropriate remedies.

The Government has committed to update the Tribunal Rules following the passage of the Bill. A key change will be to ensure that the IPT's existing practice of holding open hearings where possible is expressly permitted in the Rules themselves (which have not yet been updated to reflect this development).

The IPT has the power to appoint Counsel to the Tribunal, who ensures that all parties to a claim or complaint receive a fair hearing. Special Advocates would duplicate that role, and would introduce extra expense and delay to Tribunal proceedings.

Notification of surveillance is not required to ensure effective oversight in the UK because the IPT has an extremely wide jurisdiction. In *Kennedy v UK (*para. 167) the European Court of Human Rights (ECtHR) states: "any person who suspects that his communications have been or are being intercepted may apply to the IPT… The jurisdiction of the IPT does not, therefore, depend on notification to the interception subject that there has been an interception of his communications." The Venice Commission noted that notification is not an absolute requirement of Article 8 of the ECHR and that "if a state has a general complaints procedure to an independent oversight body, this can compensate for non-notification".

A notification requirement could require suspected criminals and terrorists to be alerted to the fact that powers had been used against them, simply because a specific on-going investigation had stalled. This would reveal sensitive capabilities and could hinder future or parallel investigations.

Notification also threatens the well-established principle of neither confirming nor denying (NCND) sensitive matters relating to national security, which is crucial to maintaining the efficacy of sensitive capabilities. The ECtHR has recognised the importance of the NCND principle (*Klass v Germany 5029/71*, *Weber* v Germany 54934/00 and *Segerstedt-Wiberg v Sweden* 62332/00). NCND protects operational capabilities but effective scrutiny is still carried out by the ISC, the Commissioners, and the IPT- who will find in favour of the complainant and provide a remedy when activity is found to be unlawful.

The Investigatory Powers Bill will provide a new power for the Investigatory Powers Commissioner – a senior, independent judge – to notify individuals who have suffered as a result of serious errors in the use of investigatory powers. It will then be open to those individuals to seek redress through the IPT.

The Bill also creates a new domestic appeal route from the IPT. Leave to appeal can be granted on any decision or determination made by the IPT where there is a point of law and the IPT or relevant appellate court considers that the appeal would raise an important point of principle or practice or there is another compelling reason for granting leave for appeal.

Section 4 of the Human Rights Act 1998 lists the courts which are able to make declarations of incompatibility. This list includes the UK's most senior courts, such as the Court of Appeal, but does not currently include any Tribunals. The creation of a domestic appeal route from the IPT will ensure that where a case is appealed to the Court of Appeal or devolved equivalent, the appellate court would have the ability to make a declaration of incompatibility under the Human Rights Act 1998. As a result, we do not consider it is necessary to extend this ability to the IPT itself.

Recommendation:

Three parliamentary committees have conducted pre-legislative scrutiny and published reports on the draft Bill in February 2016. The Commissioner commends the work of these Committees and the fact they produced 198 recommendations in the three months or so in which they had to work. However, the Commissioner has concerns with the compressed timeline for the IP Bill, which has meant that the pre-legislative scrutiny has been put under pressure.

Response:

The timeline for the Investigatory Powers Bill reflects the expectation set by Parliament during the passage of the Data Retention and Investigatory Powers Act 2014 that new legislation should be on the statute books by the end of 2016.

The Bill has been the subject of extensive Parliamentary scrutiny. The Bill itself builds on the recommendations of three independent reviews that were published between March and July 2015.

The Government published a draft Bill in response to their recommendations in November 2015. That draft Bill was subject to extensive pre-legislative scrutiny by three Parliamentary Committees. The Government introduced a revised Bill on 1 March, responding to the recommendations of those Committees.

The Bill has now had line by line scrutiny by a cross-Party Bill Committee in the House of Commons. The timetable for that Committee's work was agreed by Parliament. It will receive further scrutiny during the remaining stages in the Commons and as it progresses through second reading, committee, report and third reading in the House of Lords. Usually proceedings on Bills must be completed in a single parliamentary session, but recognising the need to ensure the Bill would be able to follow the usual legislative procedures in the two Houses, a motion to allow proceedings to carry over from the 2015–16 session and into the 2016–17 session was agreed on 15 March.

Recommendation:

The Commissioner welcomes the creation of one Investigatory Powers Commissioner who will replace the current work of three Commissioners. However, he considers that an Investigatory Powers Commission should be set up with the Investigatory Powers Commissioner as its head. Expert oversight bodies are well placed to undertake the ongoing, detailed and politically neutral scrutiny that human rights protection requires. In addition, the Commission needs to be adequately funded, with a role for Parliament given in determining that budget. Indeed, the importance of strengthening the overall link between expert oversight bodies and Parliament is emphasized in recommendation 13 of the 2015 Issue Paper on Democratic Oversight. This extends to giving a designated parliamentary committee a role in the appointment of members, empowering parliament to task expert bodies to investigate particular matters and require expert bodies to report and take part in parliamentary committee hearings. The staff of the Investigatory Powers Commissioner also needs the relevant technical expertise.

Response:

The Bill will replace the current fragmented oversight regime with a powerful Investigatory Powers Commissioner – a senior judge – who will have the support, powers, resources and technical expertise to effectively, and visibly, hold the agencies and law enforcement to account.

The Investigatory Powers Commissioner, supported by judicial commissioners and expert staff, will have responsibility for conducting inspections and investigations to ensure that powers are being used fully in accordance with the law.

The Investigatory Powers Commissioner will have increased resources, including technical, legal and communications expertise so that they are more effective and visible. They will have sufficient resources to contract any particular specialist technical expertise that they feel is necessary to perform their statutory functions.

The Investigatory Powers Commissioner will have exactly the same powers of audit, investigation and inspection as a Commission. However they will not have the bureaucracy of supporting themselves as a public body and instead will be able to focus on their core role. For this reason it is more cost efficient, but just as powerful, to create a Commissioner role instead of a Commission.

The IPC's budget will be determined by the Secretary of State, after consultation with the Investigatory Powers Commissioner. The IPC will be able to report publicly if they feel that they lack the necessary resources to undertake their work.

Recommendation:

Another issue raised by the surveillance experts was the fact that authorizing warrants and ex post-facto oversight of surveillance will be the task of the same institution. It may be preferable that these two functions should be performed by separate bodies within an Investigatory Powers Commission as recommendation 9 of the 2015 Issue Paper on Democratic Oversight suggests.

Response:

The Commissioner will undertake two distinct functions. The first of these functions will be to consider warrants authorising the use of investigatory powers. The second function will be to look at how the powers authorised under that warrant were used by the public authority as well as taking a wider system overview of the full process.

David Anderson QC and others concluded that there are considerable benefits to having a close relationship between the two functions so that Commissioners authorising warrants can understand in detail how warrants are put into practice. This reflects current arrangements within the Office of Surveillance Commissioners.

Recommendation:

The Commissioner is in favour of a system of notification when a person has been the subject of surveillance. As the European Court of Human Rights has reaffirmed in the case of Szabó and Vissy v Hungary (2016), "As soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should be provided to the persons concerned". Accordingly, he is pleased to see that Clause 198 of the revised IP Bill has been amended to allow the Investigatory Powers Commissioner to inform individuals of any serious errors which have caused significant prejudice or harm to the person concerned without having to seek agreement from IPT. Clause 199 now makes clear that the Judicial Commissioners can communicate with the IPT without consulting the Secretary of State. However, the system of error reporting could be improved; in particular the Commissioner supports the desirability of better defining the categories of relevant error and the criteria for seriousness of error in clause.

Response:

The Bill makes clear that an error is serious if the Commissioner considers that it has caused significant prejudice or harm to the person concerned. The Investigatory Powers Commissioner will be under a duty to keep the definition of a relevant error under review.

Recommendation:

As regards the appointment of the Judicial Commissioners, the Commissioners [sic] shares the views expressed that they should be appointed by a body which is independent of the executive, such as the Judicial Appointments Commission, or parliamentary committee. Having the Prime Minister appoint the Judicial Commissioners may compromise their independence and impartiality. The fact that the revised Bill provides for the Lord Chief Justice and others to be consulted on the appointment of the Judicial Commissioners is a positive step although it could go further. According to recommendation 13 of the 2015 Issue Paper on Democratic Oversight strengthening the link between expert oversight bodies and parliament increases their independence and democratic legitimacy.

Response:

The Bill requires that the Lord Chief Justice of England and Wales, the Lord President of Scotland and the Lord Chief Justice of Northern Ireland must be consulted before the Prime Minister may appoint a Judicial Commissioner. Lord Judge, the Chief Surveillance Commissioner and former Lord Chief Justice, has publicly stated that having the Prime Minister make the appointment will not have any impact upon the independence of the Commissioner.

Judicial Commissioners will be former or serving High Court Judges, or more senior, and will be entirely independent of Government. They will have already been appointed to these roles via a Judicial Appointments Commission process and so it will be unnecessary to have them repeat this. Introducing an appointment process which is unduly lengthy may well reduce the number of applicants who are willing to put themselves through it, leaving the office of the Investigatory Powers Commissioner short staffed.

The Bill provides that Judicial Commissioners can only be dismissed if they are demonstrably unfit to perform the role. This would include instances where a Commissioner receives a custodial sentence. Alternatively, both Houses of Parliament may approve a resolution to remove a Commissioner. This reflects the position for senior judges.

Recommendation:

As the Venice Commission has stated in their Report on Democratic Oversight (2007) there is an obvious advantage of requiring prior judicial authorisation for special investigative techniques, namely that the security agency has to go "outside of itself" and convince an independent person of the need for a particular measure. It subordinates security concerns to the law, and as such it serves to institutionalize respect for the law. If it works properly, judicial authorisation will have a preventive effect, deterring unmeritorious applications and/or cutting down the duration of a special investigative measure.

Response:

The Government recognises that independent authorisation and judicial authorisation in particular can be powerful safeguards for highly intrusive investigative techniques. Subsequent inspection by judicial figures also plays an important role.

Recommendation:

The Commissioner notes, however, that prior judicial authorisation is not required for a range of powers in the IP Bill that will interfere with the right to privacy. For example, there is no judicial authorisation for obtaining communications data, including privileged and confidential communications. The Commissioner recommends that judicial warranting should be the default mechanism for the authorisation of most surveillance, with only a limited number of cases which would be subject to the certification of the Secretary of State. There is growing support for the view that external authorisation should extend to untargeted bulk collection of information as well as the collection and access to communications data. However, as David Anderson QC has stated it is possible to envisage prior authorisation that is not undertaken by a judge (for example the role of the National Anti-Fraud Network) on the condition that the body in question is independent of the executive, has the relevant competence and resources to do the job.

Response:

Communications data can only be acquired where it is necessary in a specific investigation for a particular statutory purpose, and it is proportionate to what is sought to be achieved.

All applications must be made through a single point of contact (SPoC). The SPoC's role is to ensure effective co-operation between relevant public authorities and communications service providers, and to facilitate lawful acquisition of communications data. Once the application has gone through the SPoC it must be approved by a designated senior officer who must be independent of the investigation.

A detailed statutory code of practice (published alongside the Bill in draft) will set out the practices that must be followed by public authorities that acquire communications data.

Recommendation:

Another question which has been raised with the Commissioner is the extent of the judicial scrutiny which the Judicial Commissioners will exercise. The IP Bill specifies that when making the authorisation decision "the Judicial Commissioner must apply the same principles as would be applied by a court on an application for judicial review." Surveillance experts who met with the Commissioner in London expressed their concerns that limiting Judicial Commissioners to considering warrants on judicial review principles may mean that they are only able to overrule the Home Secretary if he or she is deemed to have acted unreasonably. According to this view, the 'double-lock' system is not truly judicial authorization, but rather executive authorization with approval then being given by a Judicial Commissioner. Experts expressed the view that while the flexible nature of judicial review principles means that in theory a full merits review could take place, the Judicial Commissioners may feel bound to follow the Secretary of State's view on what is necessary for the purposes of national security. While the 'double-lock' on the most intrusive warrants is an improvement on the current position, the Commissioner is concerned that the proposed system of judicial approval is not compliant with the independent authorization suggested in recommendation 6 of the 2015 Issue Paper on Democratic Oversight.

Response:

The Investigatory Powers Bill provides for a 'double lock' authorisation system for the use of the most sensitive investigatory powers. This means that a Secretary of State will need to agree that a warrant is necessary and proportionate, and then an independent Judicial Commissioner – who will be, or have been a senior judge – will have to approve that decision before the warrant can take effect.

This approach ensures that the Bill will continue to provide democratic accountability to Parliament through the role of the Secretary of State, whilst also providing for independent external judicial scrutiny of each decision made. This 'double lock' will give the UK one of the strongest oversight systems in the world.

During pre-legislative scrutiny the Joint Committee of Parliament expressed support for the 'double lock' safeguard, including the judicial review test.

The principles of Judicial Review are well established and understood by the courts. Under the proposed model, the Judicial Commissioner would have scope to consider whether the Secretary of State's decision was lawful and rational. This would include reviewing whether the Secretary of State's decision was necessary and proportionate.

If the Judicial Commissioner disagreed with the decision of the Secretary of State, the warrant would not be issued. The Bill provides for an 'appeal' mechanism by which the Secretary of State may ask the Investigatory Powers Commissioner (IPC) to reconsider the warrant. The IPC's decision would be final.

Recommendation:

Another issue which the surveillance experts raised with the Commissioner was the importance of an adversarial process. The judicial authorisation would be decided on an ex parte basis where the Judicial Commissioner would not have the opportunity of representations by lawyers acting for the person who is the subject of the surveillance measure. The Commissioner considers that introduction of security-vetted special advocates to represent the legal interests of the targets of surveillance could help to reduce the risk that approval processes simply become rubber stamping exercises. Anonymised judgments on issues of principle could also be considered.

Response:

It will be for the Secretary of State and the Judicial Commissioner to determine whether the interference with an individual's privacy is necessary and proportionate in the context of an individual warrant application. The Judicial Commissioner will act entirely independently of Government. The Judicial Commissioners will have access to their own legal experts should they wish to consult them.

Recommendation:

The Commissioner considers that Judicial Commissioners should also be able to refer matters directly to the IPT for consideration where they have identified unlawful conduct following an inspection, audit, investigation or complaint. This could be particularly useful where an issue affects a group or class of individuals who are unlikely to pursue an individual claim before the Tribunal.

Response:

Courts and tribunals do not consider and determine legal issues without a party first having issued a claim or brought proceedings. This is a fundamental principle of the UK's justice system. Where an error is serious, a Judicial Commissioner will inform the subject of the error of their right to apply to the IPT for remedy. If Judicial Commissioners were to inform the IPT of unlawful conduct they had identified, the IPT would not be empowered to take action.

Recommendation:

There is no explicit requirement in the IP Bill that the Secretary of State or a Judicial Commissioner consider the existence of a reasonable suspicion against any person prior to approving or authorising the surveillance measure. The Commissioner finds that this is problematic in light of the judgment of the Grand Chamber of the European Court of Human Rights in the case of Roman Zakharov v. Russia (2015), "Turning now to the authorisation authority's scope of review, the Court reiterates that it must be capable of verifying the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures, such as, for example, acts endangering national security." This is the case, even following the more nuanced approach in the later Chamber judgment of Szabó and Vissy v Hungary (2016).

Response:

As part of the judgement as to whether a warrant meets the test of necessity and proportionality, the Secretary of State and the Judicial Commissioner will consider all the facts of the case. The test of necessity and proportionality has been repeatedly reaffirmed as legal by European and UK courts.

Recommendation:

Parts 6 and 7 of the IP Bill deal with a range of bulk warrants. These include bulk interception warrants related to communications sent or received by individuals outside the UK; bulk acquisition warrants, related to the acquisition of communication data; bulk equipment interference warrants; and bulk personal dataset warrants.

The Commissioner notes the concerns made by the three UN Special Rapporteurs in their written evidence to the Joint Committee on the Draft Investigatory Powers Bill who found that the provisions on the bulk interception warrants are vague and not tied to specific offences. Surveillance experts also highlighted their concerns about the human rights implications of bulk collection.

Recent case law of the European Court of Human Rights is instructive in relation to bulk surveillance powers. In Zakharov v Russia (2015) the Grand Chamber held that interceptions "must clearly identify a specific person to be placed under surveillance or a single set of premises as the premises in respect of which authorisation is ordered. Such information may be made by names, addresses, telephone numbers or other relevant information". Surveillance experts suggested to the Commissioner that the sheer breadth of a bulk warrant may have difficulties against that clear standard, since the bulk interception warrants, as set out, require no specific individuals to be mentioned or specific groups, no specific telephone numbers, nor specific premises. By their nature bulk warrants place large groups of people under the menace of surveillance without any suspicion on the part of the authorities that an individual has committed a criminal offence or is of national security interest.

Given that the legality of bulk surveillance models is subject to litigation in the UK and is pending before the European Court of Human Rights, the Commissioner considers it would be premature to determine whether the regime is proportionate for the purposes of Article 8 of the ECHR. The Commissioner notes the careful analysis of this issue by the ISC, the Interception of Communications Commissioner's Office and the IPT, which laid out the full safeguards which operate to protect individual privacy. Nevertheless, the Commissioner has serious concerns as to whether generic interception of external communications is an inherently disproportionate interference with the private lives of a great number of persons.

Response:

The use of bulk powers is vital to the work of the security and intelligence agencies. None of the bulk powers in the Bill is new. The Bill will ensure that the use of bulk powers by the security and intelligence agencies will be subject to enhanced safeguards.

The Bill will place strict safeguards on the authorisation of bulk warrants. All bulk warrants will be issued by a Secretary of State and approved by a Judicial Commissioner. National security must always be one of the statutory purposes when issuing a bulk warrant.

Strict safeguards will govern access to data that has been collected in bulk. Before an analyst can access any data obtained under a bulk warrant, he or she will need to ensure that it is necessary and proportionate for a specific operational purpose that will have been approved by the Secretary of State and a Judicial Commissioner at the point the warrant was issued.

In addition, analysts will only be able to select for examination the content of communications of a person in the UK if they have obtained a targeted examination warrant from the Secretary of State, approved by a Judicial Commissioner.

On introduction of the Bill, the Government published an operational case for bulk powers, setting out in more detail than ever before how these powers are used and why they are needed. The Rt Hon Dominic Grieve MP, Chairman of the ISC stated that "the present Committee and its predecessor are satisfied that the Government are justified in coming to Parliament to seek in broad terms the powers that the Bill contains. None of the categories of powers in the Bill — including the principle of having powers of bulk collection of data, which has given rise to controversy in recent years — is unnecessary or disproportionate to what we need to protect ourselves."

Recommendation:

From a privacy point of view, equipment interference is very problematic. As one NGO has submitted, it represents, "The modern equivalent of entering someone's house, searching through his filing cabinets, diaries and correspondence, and planting devices to permit constant surveillance in the future, and, if mobile devices are involved, obtaining historical information including every location he visited in the past year … if a mobile device has been infected, the ongoing surveillance will capture affected individuals wherever they are."

The IP Bill provides for law enforcement and the security and intelligence agencies to undertake targeted equipment interference. Equipment could include personal computers, mobile phones and tablets as well as large systems owned by organisations. The Commissioner welcomes the fact that this practice, which previously took place without a detailed legal framework, is now addressed in the IP Bill.

However, he has serious concerns over the broad wording of the clause governing equipment interference. He considers that if equipment interference is used at all it must only be allowed in the most narrowly defined circumstances, when necessary and proportionate, and with the strictest safeguards. Moreover, and in line with recommendation 7 of the 2015 Issue Paper on Democratic Oversight, these activities must be subject to the same level of external oversight as is required for surveillance measures that have equivalent human rights implications.

Response:

Equipment interference is a set of techniques used to obtain a variety of data from equipment; this includes traditional computers or devices such as smart phones. Equipment interference can be carried out either remotely or by physically interacting with equipment. This is not a new power.

Law enforcement agencies currently have the power to conduct equipment interference under the Police Act 1997. The security and intelligence agencies have similar powers under the Intelligence Services Act 1994.

The Bill provides for enhanced safeguards and brings all equipment interference powers as they relate to electronic communications into one, clearer place.

The Bill will apply strong safeguards, ensuring that equipment interference is used only when necessary and proportionate, and will ensure that the data obtained from equipment interference is stored safely and once no longer required any information is destroyed securely.

The Investigatory Powers Bill will strengthen EI authorisation safeguards by introducing a 'double lock', requiring that warrants will not be issued until they have been authorised by a Judicial Commissioner.

Recommendation:

National security is given as a test of the necessity of an action for a number of powers in the IP Bill. However, the term national security is not defined in the Bill. The Commissioner is of the view that a definition of national security would be helpful in ensuring legal certainty. A lack of a clear definition allows for arbitrariness and abuse of rights.

Response:

Efforts to define national security in statute would run a real risk of restricting the ability of the UK to respond to changing circumstances. This point is well-made in the ECtHR judgment *Kennedy v UK* s 159: "By the nature of things, threats to national security may vary in character and may be unanticipated or difficult to define in advance."

Recommendation:

Surveillance experts raised the issue of legal professional privilege and journalistic privilege with the Commissioner in the context of the IP Bill. The Commissioner commends the fact that there has been some progress made on both of these fronts in the period between the draft Bill and current Bill; however professionals in this field continue to highlight their concerns.

As regards legal professional privilege, the Commissioner is concerned that powers in the IP Bill enable certain security and other agencies deliberately to target legally privileged communications. The Commissioner encourages the authorities to consult further with the Law Societies and others providing protection for Legal Professional Privilege on the face of the Bill.

The Commissioner also shares concerns that journalists and their sources are not adequately protected and supports the call for scrutiny before access is made to journalistic material. The protection of journalistic sources needs to be fully enshrined in the IP Bill to protect the whistleblowers and the journalists who report on their stories. The Commissioner recalls the Council of Europe standards on whistleblowers, such as the Committee of Ministers, of Recommendation CM/Rec(2014)7 on the protection of whistleblowers, which calls on member States to create an appropriate normative, judicial and institutional framework for the protection of whistleblowers, and the Council of Europe Parliamentary Assembly (PACE) Resolution 2060 (2015) on improving the protection of whistleblowers.

Response:

The Bill – and accompanying codes of practice – will provide strong protections for sensitive professions.

Issues surrounding the infringement of the right to freedom of expression may arise where a request is made for the communications data of a journalist. There is a strong public interest in protecting a free press and freedom of expression in a democratic society, including the willingness of sources to provide information to journalists anonymously.

Accordingly the Government recognises that requests for communications data intended to identify journalistic sources should be subject to judicial approval. The Bill puts on a statutory footing the requirement for public authorities to obtain judicial authorisation before obtaining communications data to identify a journalistic source.

The Bill also provides explicit protection for legally privileged material in relation to interception and equipment interference. This includes a requirement that the deliberate interception of legally privileged communications may only be authorised in exceptional and compelling circumstances.

Recommendation:

Reportedly around 900 children were referred to 'Channel', the Government's anti-radicalisation programme, in the three years April 2012-April 2015. In the three months June-August 2015, 312 children were referred (of 796 referrals in total).

Response:

Channel provides support for those most at risk of radicalisation. It is voluntary, and support is only provided following careful assessment by experts. The vast majority of Channel cases achieve a successful outcome, with two thirds of those who choose to participate leaving with no further concerns about their vulnerability of being drawn into terrorism.

Channel is a voluntary programme and does not constitute any criminal sanction.

Channel supports vulnerable people of any age, including young people.

Referrals to Channel can come from anyone who is concerned that someone they know is at risk of being drawn into terrorism. It is far better that people refer a person to Channel when they have genuine concerns and that person turns out not to be at risk, than for people to ignore their concerns.

All referrals are assessed by either or both a local authority Multi-Agency Safeguarding Hub and/or a Police Channel Coordinator to see if they are suitable for Channel. In many cases where Channel is not suitable, individuals have been passed to other mainstream services, such as social services, for support. For others, no further action has been taken. Feedback is provided on all referrals to Channel. We are equipping frontline professionals through Prevent training with the skills and knowledge to help them understand better the role that they can play in countering radicalisation and refer individuals they are concerned about.

Recommendation:

The UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism in his recent report to the Human Rights Council was of the opinion that, 'effective strategies should not be based on pre- or mis-conceptions about the groups that are most susceptible to radicalisation or violent extremism, but should be developed in reliance on evidence to ensure a proper understanding of the national and local issues that impact on the radicalisation process. This will not only ensure that all at-risk communities are adequately engaged with, but also that entire communities, ethnic or religious groups are not stigmatised. Certain groups of persons, namely Arabs, Jews, Muslims, certain asylum seekers, refugees and immigrants, certain visible minorities and persons perceived as belonging to those groups have become particularly vulnerable to racism and/or racial discrimination across many fields of public life as a result of the fight against terrorism. The Commissioner stresses the responsibility of all member States of the Council of Europe to ensure that the fight against terrorism does not have a negative impact on any minority group.

The Commissioner supports the fact that concrete measures should be taken to prevent and fight radicalisation, in particular in schools, disadvantaged neighbourhoods, prisons and on the Internet and social media, in line with PACE Resolution 2031 (2015) .

However, the Commissioner shares concerns that the 'Prevent' programme runs the risk of isolating the very communities whose cooperation is most needed to fight violent extremism. Reinforcing community support and gaining the confidence of communities should be the government's priority. This may be done by promoting intercultural dialogue in schools; taking measures to combat marginalisation, social exclusion, discrimination and segregation, especially among young people in disadvantaged neighbourhoods; and through supporting families in their role of educating their children to respect the values of democracy and tolerance.

Response:

Prevent is about safeguarding people who are at risk of radicalisation. Prevent does not target a specific faith or ethnic group - it deals with all forms of extremism. Rather, Prevent protects those who are targeted by terrorist recruiters.

This is challenging but absolutely necessary work. Currently the greatest threat comes from terrorist recruiters inspired by Da'esh. Our Prevent programme will necessarily reflect this by prioritising support for vulnerable British Muslims, and working in partnership with British Muslim communities and civil society groups.

Thanks to Prevent thousands of people in the UK have been safeguarded from targeting by extremists and terrorist recruiters. That includes those at risk from far-right and Neo-nazi extremism, as well as those vulnerable to Islamist extremism.

Recommendation:

Moreover, NGOs, as well as David Anderson QC, question the impact on children's rights, including freedom of speech, of the 'Prevent' programme duty in schools.28 A number of academics expressed their fear by way of an open letter in the press that the statutory implementation of the strategy through the Counter-Terrorism and Security Act 2015 would have a chilling effect on open debate, free speech and political debate.29 The Commissioner recalls that the response to the threat of terrorism should not itself encroach upon the very values of freedom, democracy, justice and the rule of law.

Response:

Keeping our children safe and ensuring our schools prepare them for life in modern, multi-cultural Britain could not be more important.

Schools already play an important role in safeguarding young people from various harms, including physical/sexual, drug abuse and bullying. Similarly school staff can also play a role in identifying the signs of radicalisation and thereby help reduce the risks of radicalisation.

Schools should be safe spaces where children and young people can challenge and discuss ideas around extremism and develop the critical thinking skills that allows them to reject extremism.

In 2014-2015 we engaged over 14,000 students and teachers through our Prevent projects that cover a range of activities, including teaching young people about the dangers of online messaging on extremism and running interactive drama workshops which provide a safe environment to discuss issues around cultural identity and extremism.

We want teachers to encourage debate about difficult issues, including radicalisation, in their classrooms, not to stifle it. To assist with this, we have provided them with advice and curriculum materials, including the Educate Against Hate online portal, launched with DfE, which also has information and helpful tools for parents, school leaders and governors.

The Duty is not about restricting debate or free speech. We have explicitly said that schools should be safe spaces in which children and young people can understand and discuss sensitive topics. That includes terrorism and the extremist ideas that are part of terrorist ideology. They need to learn how to challenge these ideas. Ideas that they see in the newspapers and on the internet every day.
The Prevent duty should not limit discussion of difficult issues. We expect schools to be proactive in challenging intolerance in the classroom and in school communities. We cannot be neutral in the face of intolerance.

Schools are already expected to promote the spiritual, moral, social and cultural development of pupils and, within this, fundamental British values. Advice on promoting fundamental British values in schools is available.