



UK Mission to the
United Nations
in Geneva

UK Mission Geneva
PO Box 6
Avenue Louis Casati 58
1216 Cointrin GE

Tel: 022 918 2363

Note No 051

The Permanent Mission of the United Kingdom of Great Britain and Northern Ireland presents its compliments to the United Nations Special Rapporteur on the rights to freedom of opinion and expression, the United Nations Special Rapporteur on the rights to freedom of peaceful assembly and of association and the United Nations Special Rapporteur on the situation of human rights defenders and has the honour to transmit the attached response to the letter from the Special Rapporteurs dated 22 December 2015 concerning the draft Investigatory Powers Bill.

The Permanent Mission of the United Kingdom avails itself of this opportunity to renew to the Special Rapporteurs the assurances of its highest consideration.

10 March 2016



UN Special Rapporteur on the rights
to freedom of opinion and expression,
UN Special Rapporteur on the rights to freedom
of peaceful assembly and of association,
UN Special Rapporteur on the situation of
human rights defenders
Office of the High Commissioner for Human Rights



Foreign &
Commonwealth
Office

King Charles Street
London SW1A 2AH

Secretary of State

9 March 2016

David Kaye, Special Rapporteur
Maina Kiai, Special Rapporteur
Michel Forst, Special Rapporteur
OHCHR
Palais des Nations
1211 Geneva 10

Dear Special Rapporteurs,

Thank you for your letter of 22 December 2015, on the Investigatory Powers Bill. The Government's intention is that the Bill should set a new standard for openness and transparency with regard to both the powers available to the United Kingdom's law enforcement and security and intelligence agencies, and how the agencies may use those powers. In all cases we recognise the need to ensure that the agencies continue to behave in a way which is compliant with our international obligations to uphold and respect human rights, and that they may be held democratically accountable for their actions. Consultation on the draft provisions of the Bill was therefore an important part of its development, and I welcome that you made a formal submission to the Joint Committee.

The timeline for the review process of the draft Bill was in response to the sunset clause attached to the Data Retention and Investigatory Powers Act 2014 (DRIPA), which means that it will expire in December 2016. The Government committed to allow Parliament the chance to discuss these powers substantively, and has met this commitment. Introduction of the Bill to the House of Commons on 1 March was to ensure sufficient time for Parliament to debate fully the provisions contained in the Bill, following the normal Parliamentary timetable.

The context of the Bill was set out by the Home Secretary in presenting the draft Bill to Parliament in November 2015, and in the Government's subsequent presentations to Parliament's Joint Committee on the Bill. Further detail is provided in the Guide to Powers and Privacy Safeguards, which sets out the key changes we have made to the Bill following pre-legislative scrutiny by three parliamentary committees, and other supporting documents available at:
<https://www.gov.uk/government/collections/investigatory-powers-bill>.

I am confident that the Bill is compatible with international law. Set out in the attached annex are responses to your specific questions. I hope that this addresses your concerns. If there is any further information you require, my officials would be happy to discuss the Bill with you.

Yours sincerely
Philip Hammond

THE RT HON PHILIP HAMMOND MP

Annex: UK Investigatory Powers Bill: response to questions on specific provisions of the draft Bill

Purposes of Warrants

Your second question asks how the purpose of authorisations for journalists' communications data, data retention notices, warrants for bulk interception and technical capability notices meets the requirements of international norms and standards, including the International Covenant on Civil and Political Rights. We are fully committed to meeting our obligations under international human rights law, and ensuring that agency activity is strictly necessary and proportionate.

The Investigatory Powers Bill replicates current legislation in restricting the statutory purposes for which relevant public authorities may use the powers available to them. Public authorities may, in addition, only use the purposes set out in the Bill in relation to the specific offences or conduct that they have been given the statutory function to investigate. Where an application for communications data is made to determine a journalistic source, there must be an overriding requirement in the public interest and the authorisation must be approved by a Judicial Commissioner. The revised Bill makes clear that this applies to the security and intelligence agencies as well as law enforcement. Each authority must keep a record of all applications, including what consideration has gone into the public interest in obtaining this data.

As for bulk interception warrants, access to bulk data is crucial to monitoring known and high priority threats and is also a vital tool in discovering new threats. Part 6 of the Bill provides for the use of interception, communications data and equipment interference powers in bulk.

There are robust safeguards in the Bill governing access to data which has been collected under bulk warrants, to ensure that it is only examined where it is necessary and proportionate to do so. The Secretary of State must always be satisfied that a bulk warrant is necessary in the interests of national security before it can be issued. Warrants must also contain specific operational purposes, which govern the circumstances under which any material that has been collected in bulk may be selected for examination. They stem from agreed HMG priorities, and must relate to one or more of the statutory purposes for which the warrant is issued. Operational purposes must be agreed by both the Secretary of State and the Judicial Commissioner when they approve a warrant application. They will provide the Secretary of State and the Judicial Commissioner with a more detailed understanding of the purposes for which material collected in bulk will be selected for examination. No material collected in bulk may be selected for examination unless doing so is necessary for one or more of the specified operational purposes.

In terms of the purposes for which data retention notices may be issued, data can only be retained where necessary and proportionate for one or more of the specific statutory purposes set out in Part 3 of the Bill. Once retained, any access to that data by law enforcement or security/intelligence agencies must also be necessary and proportionate to a specific investigation and relevant to one of the same specific statutory purposes. As you know, the Bill also creates an avenue of appeal, and extends the responsibilities of the Technical Advisory Board (TAB) to include advice

on data retention notices. This acts as an additional safeguard for Communications Service Providers (CSPs).

As you noted, the Bill also provides for technical capability notices to be given to CSPs. Regulations, subject to Parliamentary approval, will set out the obligations which may be imposed on a CSP to maintain a permanent technical capability in order to allow them to give effect to interception, equipment interference or bulk communications data (CD) acquisition warrants, or CD acquisition authorisations, quickly and securely. A technical capability notice will then impose a requirement on a particular CSP to comply with (some of) those obligations, and will set out the detailed steps which the CSP is required to take in order to do so. The provisions on technical capabilities also enable the Secretary of State to impose obligations on a CSP to maintain the ability to remove any electronic protection that they (the company which is subject to the notice) have applied to communications, or which has been applied on their behalf, when served with a relevant warrant, notice or authorisation. We recognise the importance of encryption, which keeps personal data and intellectual property secure and ensures safe online commerce. It is the foundation of a strong, internet based economy. But as technology develops at an ever increasing rate, it is only right that we make sure we keep our citizens safe. Terrorists, paedophiles and other criminals should not be able to communicate online without consequences.

The obligations in the Bill relating to encryption maintain the existing position in UK legislation. This makes clear that a company subject to a notice requiring it to maintain a permanent technical capability is required to remove electronic protection (i.e. remove encryption), and provide the content of communications in intelligible form, when they have been served with a warrant requiring them to do so. In practice, the requirement to maintain a permanent technical capability will only be placed on companies that are required to give effect to warrants on a recurrent basis and only following consultation with the company themselves. Such obligations will only relate to the removal of electronic protections that a company has itself applied to communications, or which have been applied on its behalf. This ensures that companies can access the content of communications on their networks when presented with a lawful authorisation to do so, as many of them already do for their own business purposes, for example to target advertising. A notice cannot authorise or require a CSP to disclose communications or communications data in the absence of an appropriate warrant or authorisation.

As with data retention notices, CSPs have an avenue of appeal in relation to technical capability notices. In considering any appeal, the Secretary of State must consult both the TAB for its view on the technical feasibility and cost of the notice, and the Investigatory Powers Commissioner for his/her view on whether the obligations imposed by the notice are reasonable.

Right of Appeal and Remedy

Your third question asks how the right to appeal and the right to an effective remedy are promoted and protected in relation to the lack of disclosure of authorisations for journalists' communications data or warrants for bulk interception and technical capability notices, and how the draft Bill complies with international norms and standards. Disclosures of requests for communications content or communications

data would risk undermining national security and the prevention and detection of crime. However, CSPs will be able to disclose the existence of a request made for a person's communications data where the public authority gives them permission to do so.

All the powers in the Bill will be subject to oversight by the Investigatory Powers Commissioner and the Investigatory Powers Tribunal (IPT). The IPT has a broad jurisdiction to consider any complaint which alleges wrong-doing by a public authority, including the security and intelligence agencies, involving the use of investigatory powers. In recognition of the fact that warrants and notices cannot be disclosed, there is no requirement for the complainant to have evidence of the alleged wrong-doing. It is sufficient that they believe that covert activity has taken place. The IPT is able to investigate, obtain and protect evidence on behalf of all parties to a complaint. All public authorities are under a statutory obligation to provide the IPT with anything it requires in the course of its investigation. The Bill will also strengthen the ability to challenge suspect or illegal surveillance, by creating a domestic right of appeal for the IPT's decisions.

Judicial Oversight

Your fourth question asks how authorisations for journalists' communications data or warrants for bulk interception, data retention notices and technical capability notices have the requisite independent judicial oversight to meet with international norms and standards. We do not believe that the appointment process will compromise the independence and impartiality of the Judicial Commissioners. The revised Bill makes clear that the Prime Minister must now consult with the Scottish Government, Northern Ireland Executive, the Lord Chief Justice and his equivalents in the Devolved Administrations before appointing the Investigatory Powers Commissioner. Furthermore, the Prime Minister must consult all those named above, and the Investigatory Powers Commissioner, before appointing other Judicial Commissioners.

Likewise, the ECHR emphasised the independence and impartiality of the IPT in their ruling on *Kennedy v. UK*. Application No. 26839/05.

On whether the review process of data retention and technical capability notices provides independent oversight, we believe that the final authority in decisions relating to national security should rest with the executive, in recognition of the fact that the executive holds the expertise in balancing the interest of national security against other public interest considerations. It is a well established principle that the judiciary should therefore accord the executive with a wide margin of appreciation in this area. Consultation between the Secretary of State, the TAB and Investigatory Powers Commissioner will be required under the proposed legislation, and the Secretary of State must act within the law.

In addition, the Investigatory Powers Commissioner will have oversight of the operation of the data retention provisions in the Bill, and these provisions are now also within scope of the IPT's functions. We consider that these oversight arrangements will provide significant reassurance on the data retention provisions.

You raised the issue of time limits on bulk interception warrants. Given the challenges in maintaining national security in the modern world, we believe it would be artificial to impose an arbitrary limit on the number of times a warrant can be renewed, and would reduce operational effectiveness. Whenever a warrant is renewed the 'double-lock' authorisation will apply, requiring the Secretary of State and a Judicial Commissioner to be satisfied that the activity described in the warrant remains necessary and proportionate in the interests of national security. Bulk interception warrants will only be issued where the information cannot be obtained by other means.

Journalistic Information

Finally, you express concern regarding the boundaries of the proposed definition of "a source of journalistic information". This includes any source of journalistic information, wherever that may originate. I understand your concerns about the potential impact on freedom of expression and association, and would emphasise what I have said above about the need for an overriding requirement in the public interest and approval by a Judicial Commissioner before an authorisation can go ahead.

Retention of Communications Data

In your letter you also refer to the prohibition on disclosure of data retention notices by CSPs. This does extend to statistics on the number and type of notices that they receive, that they send back for review, and which are modified, varied or revoked. It has long been the practice of Governments not to disclose the existence of data retention notices. Disclosing the existence of a notice would risk undermining national security and the prevention and detection of crime. For example, criminals might start to use the services of companies that are not subject to a notice. The commercial interests of that company could be prejudiced if the Government made the fact of a notice public and significant numbers of customers transferred their business to companies who are not subject to a notice.

The Investigatory Powers Commissioner will consider what, if any, statistics should be published on data retention notices. It is also worth noting that the Bill provides for the giving of data retention notices to come under the IPT's jurisdiction.