HOUSE OF COMMONS

4 April 2012

Dear Colleague

There has been a lot of press coverage in recent days about two of our key policies to maximise public protection: on communications data capability and the Justice and Security Green Paper. We are committed to maintaining national security and protecting the public in the face of changing circumstances whilst continuing to honour our commitment to protect civil liberties.

1. Communications data capability

The need to act

Communications data – information such as who called whom and at what time – is vital to law enforcement, especially when dealing with organised crime gangs, paedophile rings and terrorist groups. It has played a role in every major Security Service counter-terrorism operation and in 95 per cent of all serious organised crime investigations. Communications data can and is regularly used by the Crown Prosecution Service as evidence in court.

But communications technology is changing fast, and criminals and terrorists are increasingly moving away from landline and mobile telephones to communications on the internet, including voice over internet services, like Skype, and instant messaging services. Data from these technologies is not as accessible as data from older communications systems which means the police and Security Service are finding it increasingly hard to investigate very serious criminality and terrorism. We estimate that we are now only able to access some 75% of the total communications data generated in this country, compared with 90% in 2006. Given the pace of technological change, the rate of degradation could increase, making our future capability very uncertain.

That is why, in the Government's Strategic Defence and Security Review, published in 2010, we said we would "introduce a programme to preserve the ability of the security, intelligence and law enforcement agencies to obtain data and to intercept communications within the appropriate legal framework."

We therefore propose to require internet companies to collect and store certain additional information, like who an individual has contacted and when, which they may not collect at present. The information will show the context – but not the content – of communications. So we will have for internet-based communications what we already have for mobile and landline telephone calls.

Safeguarding civil liberties

When we published the Defence and Security Review, we also made clear that we would "put in place the necessary regulations and safeguards to ensure that our response to this technology is compatible with the Government's approach to information storage and civil liberties." In seeking to ensure our law enforcement agencies continue to retain capabilities to protect us from harm, civil liberties will be respected and protected.

The data will be stored by the industry to enhanced standards which we shall set and which will be overseen by the Information Commissioner. The data will be available only to designated senior officers, on a case-by-case basis, authorised under the Regulation of Investigatory Powers Act (RIPA), and the process will be overseen by the Interception of Communications Commissioner. It will be available only if it is necessary and proportionate to a criminal investigation. The majority of the data will be retrospective not real time (an exception might be the tracking of a communications device during a terrorist operation or kidnapping) and will be used as part of an investigation to identify key facts, including as evidence in courts. **The police and other agencies will have no new powers or capabilities to intercept and read emails or telephone calls and existing arrangements for interception will not be changed. We envisage no increase in the amount of interception as a result of this legislation.**

Differences with Labour's proposals

Despite what has been claimed by some, this is very different to the scheme proposed by the last government. They wanted to build a Big Brother database with all communications data held in one place by government. Under our proposals, there will be no government database and the data recorded will be strictly limited and regulated and will be destroyed after a year.

The data will not be stored by the police or government but by communications service providers who already store some of this data for their own business purposes and under the EU Data Retention Directive. They will be paid by government for this service. But the costs incurred are a fraction of those we would face if we had to try to find an alternative way of developing the very significant evidence that this data provides us; indeed there is no like-for-like alternative.

We have already made changes to limit who can access communications, and how they can access it, and we intend to make further changes in future. Local authorities will now have to get a magistrate's approval to see communications data and they will not be permitted to see more than simple data, such as subscriber to a mobile phone. We intend to ensure that all departments who can get access to any data will only be able to do so under one legal framework, set out in RIPA. Access to communications data will be overseen by the Interception of Communications Commissioner. So this is not, as some have tried to suggest, a transfer of power from the judiciary to the state.

The police and Security Service will not be able to intercept the content of calls and emails, except as now when it is necessary and proportionate as part of an investigation relating to serious crime or national security, and only when they have obtained a warrant signed by a Secretary of State.

A balanced approach

For the first time in more than a decade, we have a government that respects civil liberties. We have abolished ID cards, cut back government databases and limited pre-charge detention. But we must not allow the internet to become an unpoliced space, with criminals free to go about their business with abandon.

The Government's Strategic Defence and Security Review – in which we announced our intention to update communications data capability in October 2010 – can be found here.

2. Justice and Security Green Paper

These proposals aim to find a proportionate solution to a genuine problem in a very small number of civil cases. They aim to strengthen Parliamentary oversight of the security services, and to extend justice by ending the situation in which judges cannot hear highly sensitive intelligence evidence, even where it is absolutely central to a civil court case.

The problem

British intelligence agents obviously cannot give evidence in open court about their sources, their techniques and their secret knowledge. But under current rules, the only way of dealing with information which is too sensitive to disclose is to exclude it from the court through a procedure known as Public Interest Immunity (PII). The court has no power to hear the evidence at all, even in closed session. This is a serious problem as it leaves the public with no independent judgment on very serious allegations.

A relevant recent case of this was that of the Guantanamo Detainees. The material on which the Government needed to rely to disprove the allegations of mistreatment made by the detainees was highly sensitive intelligence material which couldn't be given in open court. Since the court could not hear the evidence in closed session, they had to exclude it entirely from the case. As a result the Government was forced to stop defending itself, the public got no independent judgment on the very serious allegations, and the Government had to pay out large sums of taxpayers' money in compensation to the claimants.

The Government also faces a problem with challenges to executive decisions, for example when it refuses British citizenship or excludes from the UK an individual believed to be involved in activities which threaten national security. These decisions are made on the basis of sensitive intelligence. In judicial reviews of such decisions, again, there is no statutory basis for closed material procedures to be available to the court. This means the Government is unable to fight the case and may have to allow British citizenship to an individual believed to be engaged in terrorism-related activity, for example, because the courts have no secure forum to handle the appeal process.

Our proposals

These examples illustrate the compelling case for changing the current rules so that these sorts of cases can be properly heard in a Closed Material Proceeding (CMP) by a judge, where a judgment can be reached on the basis of all of the facts of the case, instead of a partial account; and no money paid out or decision overturned unless the Government was actually found to be at fault.

The circumstances in which a CMP would be triggered would be exceptional and rare. They will not apply at all to criminal proceedings and would only apply in compensation cases, or other civil cases based on highly sensitive intelligence material.

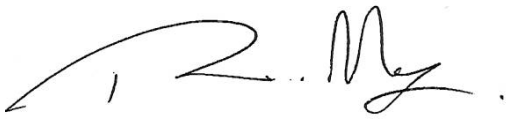
Alongside these proposals to extend judicial scrutiny over Government actions, we also want to give Parliament greater powers of scrutiny by increasing the status, remit and powers of the Intelligence and Security Committee. One option in the Green Paper is for the ISC to be made a statutory Committee of Parliament, to allow it to hold public evidence sessions and to give it the power to require information from the security and intelligence agencies.

The overall effect is that the Security Service will be more accountable to Parliament and to the courts than at present and that more sensitive evidence will be considered by courts than is possible now.

The Green Paper can be found here.

Further information

We will listen to those who have made suggestions as we develop our plans. If you require any more information, please do get in touch with our PPSs Edward Timpson MP and Ben Wallace MP.



Theresa May **Kenneth Clarke**