

Oral statement to Parliament

Home Secretary: Publication of draft Investigatory Powers Bill

From: Home Office (<https://www.gov.uk/government/organisations/home-office>) and The Rt Hon **Theresa May MP** (<https://www.gov.uk/government/people/theresa-may>)

Delivered on: 4 November 2015

Location: House of Commons

First published: 4 November 2015

Part of: Counter-terrorism (<https://www.gov.uk/government/policies/counter-terrorism>) and Policing (<https://www.gov.uk/government/policies/policing>)

Theresa May outlines commitment to providing new law on investigatory powers.



With permission Mr Speaker, I would like to make a statement about the draft Investigatory Powers Bill and our commitment to providing a new law consolidating and updating our investigatory powers, strengthening the safeguards, and establishing a world-leading oversight regime.

We live in a digital age. Technology is having a profound effect on society. Computers are central to our everyday lives. Big data is reshaping the way we live and work. The internet has brought us tremendous opportunities to prosper and interact with others.

But a digital society also presents us with challenges. The same benefits enjoyed by us all are being exploited by serious and organised criminals, online fraudsters and terrorists.

The threat is clear. In the past twelve months alone six significant terrorist plots have been disrupted here in the UK, as well as a number of further plots overseas.

The frequency and cost of cyber attacks is increasing, with 90% of large organisations suffering an information security breach last year.

And the Child Exploitation and Online Protection Command estimate that there are 50,000 people in this country downloading indecent images of children.

The task of law enforcement and the security and intelligence agencies has become vastly more demanding in this digital age. It is right, therefore, that those who are charged with protecting us should have the powers they need to do so. But it is the role of government and Parliament to ensure that there are limits to those powers.

So let me be clear, the draft Bill we are publishing today is not a return to the draft Communications Data Bill of 2012.

It will not include powers to force UK companies to capture and retain third party internet traffic from companies based overseas. It will not compel overseas communications service providers to meet our domestic retention obligations for communications data. And it will not ban encryption or do anything to undermine the security of people's data. And the substance of all of the recommendations by the Joint Scrutiny Committee which examined that draft Bill have been accepted.

So today's Bill represents a significant departure from the proposals of the past.

Today, we are setting out a modern legal framework which brings together current powers in a clear and comprehensible way. A new Bill that provides some of the strongest protections and safeguards anywhere in the democratic world. And an approach that sets new standards for openness, transparency and oversight.

This new legislation will underpin the work of law enforcement and the security and intelligence agencies for years to come. It is their licence to operate – with the democratic approval of Parliament – to protect our national security and the public's safety.

Process

Mr Speaker, this Bill responds to three independent reviews published earlier this year: the first from the Intelligence and Security Committee of Parliament; the second from David Anderson QC, the Independent Reviewer of Terrorism Legislation; and the third from the Independent Surveillance Review convened by the Royal United Services Institute.

All three reviews made clear that the use of investigatory powers is vital to protecting the public. They all endorsed the current powers available to the police and law enforcement agencies as both necessary and proportionate. And they all agreed that the legal framework governing those powers needed updating.

While considering those reviews we have engaged with technical experts, academics, civil liberties groups and communications service providers in the UK and overseas. And I also met charities supporting people affected by the crimes that these powers are used to investigate.

Mr Speaker, copies of the draft Bill will be available in the Vote Office. Our proposals will now be subject to further consultation and pre-legislative scrutiny by a Joint Committee of Parliament.

A revised Bill will then be introduced to Parliament in the spring, where it will receive careful Parliamentary scrutiny.

As the House knows, the Data Retention and Investigatory Powers Act contains a sunset clause which means that legislation will cease to have effect from 31st December 2016. It is our intention to pass a new law before that date.

What the Bill sets out

Mr Speaker, this Bill will govern all of the powers available to law enforcement, the security and intelligence agencies and the armed forces to acquire the content of communications or communications data.

These include:

the ability to retain and acquire communications data to be used as evidence in court and to advance investigations;

- The ability to intercept the contents of communications in order to acquire sensitive intelligence to tackle terrorist plots and serious and organised crimes;
- The use of equipment interference powers to obtain data covertly from computers;
- And the use of these powers by the security and intelligence agencies in bulk to identify the most serious threats to the UK from overseas and to rapidly establish links between suspects in the UK.

It cannot be right that today the police could find an abducted child if the suspects were using mobile phones to coordinate their crime, but if they were using social media or communications apps then they would be out of reach. Such an approach defies all logic and ignores the realities of today's digital age.

So this Bill will also allow the police to identify which communications services a person or device has connected to – so called internet connection records.

Mr Speaker, some have characterised this power as law enforcement having access to people's full web browsing histories. Let me be clear – this is simply wrong. An Internet Connection Record is a record of the communications service that a person has used, not a record of every web page they have accessed.

So, if someone has visited a social media website, an Internet Connection Record will only show that they accessed that site, not the particular pages they looked at, who they communicated with, or what they said. It is simply the modern equivalent of an itemised phone bill.

Law enforcement agencies would not be able to make a request for the purpose of determining – for example – whether someone had visited a mental health website, a medical website or even a news website.

They would only be able to make a request for the purpose of determining whether someone had accessed a communications website, an illegal website or to resolve an IP address where it is necessary and proportionate to do so in the course of a specific investigation.

Strict limits will apply to when and how that data can be accessed – over and above those safeguards that apply to other forms of communications data. And we will ban local authorities from accessing such data.

Transparency and oversight

Mr Speaker, I have announced today our intention to ensure that the powers available to law enforcement and the agencies are clear for everyone to understand. And the Transparency report that I am publishing today will help, and copies of that report will be available in the Vote Office. But there remain some powers that successive governments have considered too sensitive to disclose for fear of revealing capabilities to those who mean us harm.

I am clear that we must now reconcile this with our ambition to deliver greater openness and transparency.

So the Bill will make explicit provision for all of the powers available to the security and intelligence agencies to acquire data in bulk. That will include not only bulk interception provided under the Regulation of Investigatory Powers Act and which is vital to the work of GCHQ, but also the acquisition of bulk communications data, both relating to the UK and overseas.

This is not a new power. It will replace the power under Section 94 of the Telecommunications Act 1984, under which successive governments have approved the security and intelligence agencies' access to such communications data from communication service providers.

This has allowed them to thwart a number of attacks here in the UK. In 2010, when a group of terrorists were plotting attacks in the UK, including on the London Stock Exchange, the use of bulk communications data played a key role in MI5's investigation. It allowed investigators to uncover the terrorist network and to understand their plans. This led to the disruption of their activities and successful convictions against all of the group's members.

I have also published the agencies' handling arrangements relating to this power, which set out the existing robust safeguards and independent oversight. These make clear that the data does not include the content of

communications or internet connection records. The Bill will put this power on a more explicit footing and it will be subject to the same robust safeguards that apply to other bulk powers.

Oversight

The House will know that the powers I have described today are currently overseen by the Interception of Communications Commissioner, the Intelligence Services Commissioner and the Chief Surveillance Commissioner – all of whom are serving or former senior judges.

This regime worked in the past, but I am clear we need a significantly strengthened regime to govern how these powers are authorised and overseen. So we will replace the existing oversight with a powerful and independent Investigatory Powers Commissioner. This will be a senior judge, supported by a team of expert inspectors with the authority and resources to effectively, and visibly, hold the intelligence agencies and law enforcement to account. These will be world-leading oversight arrangements.

Authorisation

Finally, Mr Speaker, I want to turn to authorisation. Authorising warrants is one of the most important means by which I and other Secretaries of State hold the security and intelligence agencies to account for their actions. In turn, we are accountable to this House – and through its elected representatives – to the public

As the House knows, the first duty of Government is the protection of the public – and it is a responsibility this government takes extremely seriously.

While there was a good deal of agreement in the three independent reviews I have referenced, all three reached different conclusions on the question of who should authorise interception warrants.

The Intelligence and Security Committee supported authorisation by a Secretary of State. David Anderson said judges should carry out the authorisation. And RUSI said the authorisation of warrants should have a judicial element, but also recognised the important role of the Secretary of State.

I have considered the very good arguments put forward by the three reviews. My response is one that I hope the House agrees will provide the reassurance of both democratic accountability and judicial accountability.

So, as now, the Secretary of State will need to be satisfied that an activity is necessary and proportionate before a warrant can be issued. But in future, the warrant will not come into force until it has been formally approved by a judge.

This will place a “double lock” on the authorisation of our most intrusive investigatory powers. Democratic accountability, through the Secretary of State, to ensure our intelligence agencies operate in the interests of the citizens of this country, and the public reassurance of independent, judicial authorisation.

This will be one of the strongest authorisation regimes anywhere in the world.

And for Parliamentarians we will go even further. This Bill will for the first time put into law the Prime Minister’s commitment that in any case where it is proposed to intercept the communications of a Parliamentarian – including members of this House, members of the House of Lords, UK MEPs and the members of the devolved legislatures – the Prime Minister would also be consulted.

Conclusion

Mr Speaker, the legislation we are proposing today is unprecedented. It will provide unparalleled openness and transparency about our investigatory powers. It will provide the strongest safeguards and world-leading oversight arrangements. And it will give the men and women of our security and intelligence agencies and our law enforcement agencies – who do so much to keep us safe and secure – the powers they need to protect our country.

And I commend this statement to the House.

Share this page

- Share on Facebook (<https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.gov.uk%2Fgovernment%2Fspeeches%2Fhome-secretary-publication-of-draft-investigatory-powers-bill>)
- Share on Twitter (<https://twitter.com/share?url=https%3A%2F%2Fwww.gov.uk%2Fgovernment%2Fspeeches%2Fhome-secretary-publication-of-draft-investigatory-powers-bill&text=Home%20Secretary%3A%20Publication%20of%20draft%20Investigatory%20Powers%20Bill>)