CTSBill@homeoffice.x.gsi.gov.uk

# Counter-Terrorism and Security Bill

**Top Lines**

- Communications data – the who, where, when and how of a communication, but not its content – is a vital tool in the investigation of crime and safeguarding the public where it is necessary and proportionate for law enforcement to have access to it.
- However, there are gaps in communications data capability that have a serious impact on the ability of law enforcement to carry out their functions. One such gap is Internet Protocol (IP) address resolution.
- IP resolution is the ability to identify who in the real world was using an Internet IP address at a given point in time. An IP address is automatically allocated by a network provider to a customer's internet connection so that communications can be routed backwards and forwards to the customer.
- Communications service providers (CSPs) may share IP addresses between multiple users. The providers currently often have no business purpose for keeping a log of which device used each address.
- Therefore, as there is no existing legal requirement for CSPs to keep a log of devices and addresses, it is not always possible for law enforcement agencies to identify through their enquiries who was using an IP address at any particular time.
- This legislation will amend the Data Retention and Investigatory Powers Act 2014. This will enable the Government to require CSPs under a data retention notice to retain data that can be used to link a specific device or individual to an IP address. This data will only be available to those public bodies who are entitled to it for lawful purposes, where it is necessary and proportionate to do so on a case-by-case basis.
- These provisions will be limited and will not enable the retention of 'weblogs' – a record of information relating to a communication between a user and the internet, including the interaction with other computers connected to the internet such as those which provide an internet communication service.

**Background**

- Enabling access to data required for IP resolution will help law enforcement keep pace with the technology which is now part of our everyday lives, to answer the who, when, how, from where and with whom questions in the investigative jigsaw.
- Every user of the internet is assigned a unique identifier, or IP address. Sometimes these are static – assigned specifically to a particular device, such as a broadband router located in a home or company, and thus it is relatively easy to identify which real world identity is associated with which IP address. However, some IP addresses are shared and allocated dynamically.
- The Bill will enable us to require providers to collect and retain this data, allowing law enforcement agencies to resolve an IP address to a person in the real world.
- Without this data, it is not always possible to attribute a particular action on the internet to an individual person. For example, if a server hosting child pornographic images was seized, IP resolution would allow the police to trace the individuals who accessed the images where the server holds a log of the IP addresses and the times they were used.

**Key facts**

- Communications data has played a significant role in **every Security Service counter terrorism operation** over the last decade.
- It is used in **95% of serious and organised crime investigations** handled by the Crown Prosecution Service.

*"We accept that if communication service providers [CSPs] could be required to generate and retain information that would allow IP addresses to be matched to subscribers this would be of significant value to law enforcement. We do not think that IP address resolution raises particular privacy concerns."*
**Joint Committee on the Draft Communications Data Bill, Dec 2012**

*"Communications data is still overwhelmingly the most powerful tool available to those investigating child sexual exploitation and identifying and safeguarding its victims and potential victims."*
**Keith Bristow, Director-General, National Crime Agency, June 2014**

CTSBill@homeoffice.x.gsi.gov.uk

# Counter-Terrorism and Security Bill

**What is Communications Data and why is it important?**

- Communications data (CD) is the information about a communication. This data can help identify who has made a communication, when, where and how. It can include the time and duration of a phone call, the phone number or email address which has been contacted and the location from which a call has been made.
- CD does not include the content of any phone call or email.
- CD is used in 95% of serious and organised crime investigations handled by the CPS.
- CD has been used in all major counter terrorism investigations handled by the Security Service in the last 10 years.

**What is an IP address?**

- When a person accesses the internet they are allocated an internet protocol address by their communications service provider. This means that providers know which data should go to which customer, and route it accordingly.

**What is IP address resolution?**

- IP addresses can be shared between multiple users. IP address resolution is the process of identifying who used an IP address at a given point in time which can then be used to identify who has accessed a particular service or website.

**Why is legislation required?**

- In order to identify who used which address, CSPs need to keep data which shows which device used which IP address and at which point in time. At present they don't. This Bill would require CSPs to retain this information, which otherwise they might not do.
- The capability gap in this area is increasingly undermining the ability of law enforcement and the agencies to use communications data to keep us safe.

**Are you just reintroducing the Draft CD Bill?**

- No. These provisions will be limited to data to be retained by UK service providers which is required for IP resolution and will not include the full package of data that was covered under our previous proposals(for example, data identifying which websites are visited by individuals).

**How long will IP data be retained for?**

- The data can be retained by those CSPs under a retention notice for a maximum of 12 months.

**Will the provisions be sunsetted?**

- These provisions amend the Data Retention and Investigatory Powers Act 2014 (DRIPA). They will therefore fall at the end of 2016.

**What safeguards apply to communications data?**

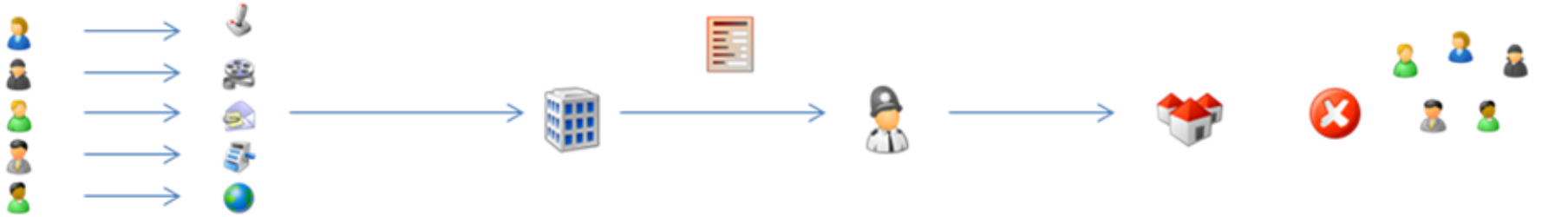
- Data retained under DRIPA will soon only be accessed using the Regulation of Investigatory Powers Act 2000 (RIPA) or a court order.
- RIPA stipulates that access to communications data is limited to the statutory purposes set out in that Act.
- Each application to access communications data has to be made individually, usually in writing and contain an explanation of why each element of the statutory requirements is fulfilled;
- Each application is scrutinised by an appropriate manager who considers the proportionality of the individual application;
- The public authorities legally permitted to request data are subject to inspection by the Interception of Communications Commissioner, who is independent from Government. Larger public authorities are subject to annual inspection;
- The Commissioner also obtains information from CSPs to audit their disclosures and ensure they correlate with the public authorities' requests.

**Is future legislation on this issue still needed?**

- As acknowledged by the Intelligence and Security Committee of Parliament during scrutiny of the Draft Communications Data Bill, there is a need for legislation to address ongoing gaps in capability which this narrow provision will not fill.
- The Prime Minister has stressed the importance of continuing to make the case for legislation and the sunset provisions in DRIPA mean that we will need to revisit this issue early in the next Parliament.
- The Government remains committed to ensuring that the police and others will have the powers they need to do their duty, protecting the public. We cannot let cyberspace become a haven for criminals.
- The Independent Reviewer of Terrorism Legislation, David Anderson QC, is carrying out a review of investigatory powers and will report by 1 May 2015.

# Counter-Terrorism and Security Bill

## Before the legislation



At 4pm 2,500 people are using a single IP address on the internet. Some are surfing the web or shopping, others are playing online games. One of those people sends illegal images by email.

The sender of the illegal email has provided limited/false details to the email service provider who therefore cannot identify who owns the account. The email service provider provides police with the IP address used by to send the email and approximate time.

Police seek details from internet access provider.

Internet access provider unable to identify which of the 2,500 people using the IP address at approximately 4pm sent the email.

Sender of the email not identified.

## After the legislation

At 4pm 2,500 people are using a single IP address on the internet. Some are surfing the web or shopping, others are playing online games. One of those people sends illegal images by email.

The sender of the illegal email has provided limited/false details to the email service provider who therefore cannot identify who owns the account. The email service provider <u>now</u> provides police with IP address and port number used to send the email and accurate time.

Police seek details from internet access provider.

Internet access provider <u>now</u> identifies the individual using the unique combination of IP address and port number provided at 4pm.

Sender of the email identified and arrested.