Local Government Association briefing
Investigatory Powers Bill, House of Commons Committee Stage
Thursday 14 April 2016

Briefing

Local Government House, Smith Square, London SW1P 3HZ
Contact: Rachel Phelps, Public Affairs and Campaigns Advisor
E-mail: Rachel.Phelps@local.gov.uk Tel 020 7664 3119

Key messages

- The LGA supports the Investigatory Powers Bill as it proposes to retain councils' access to communications data, as set out in Clauses 53 and 64. We also support Clause 223 which introduces the new definitions of communications data with 'entities' and 'events' data replacing subscriber, service use and traffic data.

- **We therefore oppose amendments 238, 239 and 240 to Clauses 64, 65 and 66** of the Bill tabled by Joanna Cherry MP (SNP, Edinburgh South West) and Gavin Newlands MP (Paisley and Renfrewshire North, SNP). These would remove local authorities from the list of relevant public bodies who would be entitled to access communications data. As such, these amendments would prevent local authorities from tackling a range of criminal activity and fraud. If councils do not have access to communications data, it should not be assumed that police forces would have the capacity to take this work on from trading standards teams.

- Although they are not the main users of communications data, teams within councils, such as trading standards, use communications data to tackle a range of criminal activity and fraud. It is vital that the powers to access communications data set out in Clauses 53 and 64 keep pace with the technology through which an increasing amount of criminal activity is perpetrated, and that councils continue to retain these powers.

- Councils will remain subject to more stringent oversight than any other body accessing communications data due to the requirement for them to seek judicial authorisation before accessing communications data. The LGA supports the safeguards identified in Clause 66 as an important means of ensuring public confidence. We are calling for the process of judicial authorisation to be more efficient so that it does not hinder appropriate use of communications data by councils.

Further information

The Office of National Statistics have reported that in the year ending September 2015, more than 600,000 fraud offences were reported in England and Wales.[i] This was an increase of five per cent compared to the previous year. This provides a partial overview, as we know some fraud offences are not reported to trading standards, Action Fraud or the police.

Local authorities have an important role in protecting consumers and businesses from fraud and similar types of criminal activity. Often those involved, like rogue traders and loan sharks, prey on the most vulnerable in society.

Communications data is used by local authority trading standards teams to tackle scams and other activities that defraud businesses and consumers. This ranges from doorstep crime which targets vulnerable and elderly people to large scale cybercrime which is often conducted remotely. While trading standards teams

sometimes work alongside the police in these cases, these are crimes that trading standards are often responsible for dealing with locally, regionally and nationally, and it should not be assumed that police services would have the capacity to deal with them if trading standards were prevented from doing so.

Charities who work with victims who are most at risk from these types of scams have endorsed the importance of councils retaining the right to access communications data. For example Age UK states: 'We know that scams are a huge and under-reported problem – recent ONS statistics estimated over 5 million incidents of fraud in a year. We also know that fraudsters target older people, exploiting those who live with dementia or are lonely. Some people are so lonely that they welcome the human contact in the scam letters they receive, or can be persuaded to trust people who turn up at the door offering to fix a problem for them, not realising them to be fraudulent. In this context, trading standards officers have an essential role to play in protecting older people. If we want to tackle this growing threat to people's wealth and health, we need to ensure councils have all the tools they need. Failure to do this means leaving older people open to continual attack and, ultimately, more pressure on the state, with victims who lose everything potentially needing health and care services and welfare benefits'.

Corporate fraud teams in councils also use communications data to prevent fraud against local taxpayers, for example, tenancy fraud, right to buy fraud, social care fraud, insurance fraud and procurement fraud.

The importance of councils being able to access communications data has also been endorsed outside of local government. The Independent Reviewer of Terrorism Legislation (IRTL) concluded in a report last year that communications data is "properly and productively used… in combating a wide range of other crimes, most of them more prevalent than terrorism and some of them just as capable of destroying lives."

Although it is extremely important that councils maintain their right to access communications data in order to undertake their work, it should be noted that councils are not the primary users of communications data. The most recent Report of the Interception of Communications Commissioner noted that councils were responsible for just 0.4 per cent of all notices and authorisations to access communications data in 2014. [1]

The LGA supports the powers set out in the Investigatory Powers Bill, which maintain councils ability to access communications data under the new definitions of 'entity' and 'events' data.

Definitions of 'entity' and 'events' data

Entity data means any data which is about 'an entity, an association between a telecommunications service and an entity, or an association between any part of a telecommunication system and an entity.'

Events data means any data which 'identifies or describes an event (whether or not by reference to its location) on, in or by means of a telecommunication system where the event consists of one or more entities engaging in a specific activity at a specific time'. The LGA has called for the Government to ensure that there is full clarity about the types of data falling within each two new definitions, so that there is a clear and transparent process for accessing each.

Safeguards and offences

We recognise there is a need for a range of safeguards to provide public reassurance that councils use communications data appropriately. We know that under existing safeguards only 19 out of 6,000 (0.3 per cent) council applications to access communications data were refused by magistrates between 2012 to 2015. These current safeguards demonstrate that the powers to access communications data are being used proportionately.

In his recent report, the IRTL suggested that current safeguards are deterring councils from seeking access to communications data.[1] Although the existing safeguards should be maintained, we agree that there is a need to ensure that they are implemented in an efficient way that does not deter appropriate use of communications data.

Central government should ensure that councils are able to apply for and be granted magistrates approval electronically, in line with the recent Spending Review commitment to fully digitise the court system. [ii] Currently, a council officer may spend several hours travelling to and from court and waiting for a physical copy of a request to be authorised.

Central government should also consider the case for routing all such applications through a small number of magistrates courts with direct links to the National Anti-Fraud Network. By creating centres of expertise, this would ensure that this safeguard is applied consistently and robustly. There are already a number of safeguards attached to councils' access to communications data, specifically the requirements that it is:

- authorised by a director, head of service or service manager (or someone who holds a higher position),
- managed through the National Anti-Fraud Network, and,
- approved by a magistrates court.

Given these checks, it is unlikely that the proposed offence of unlawfully obtaining communications data could be incurred without deliberate intent to deceive, an action which might already be covered by existing offences such as misconduct in public office. The new offences of knowingly or recklessly acquiring communications data need to be very clearly defined within the Bill to distinguish between a genuine mistake and deliberate action. Furthermore it must be clear what the legal responsibilities and consequences are for inappropriate acquisitions submitted by an applicant, undertaken by a Single Point of Contact (SPOC) and authorised by a Designated Senior Officer (DSO).

Although we do not believe the new offences are strictly necessary, we recognise the intention to provide public assurance about proper use of the powers through the creation of a specific offence. We are confident that there will not be a need to invoke the offences proposed at Clause 9 of the Bill, for unlawfully obtaining communications data, in relation to council officers.

---

[i] Office for National Statistics crime statistics September 2015 available here: http://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingseptember2015#fraud

1 Further information on the Report of the Interception of Communications Commissioner http://iocco-uk.info/docs/IOCCO%20Report%20March%202015%20(Web).pdf

[2] Further information on the Spending Review, paragraph 2.147 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/479749/52229_Blue_Book_PU1865_Web_Accessible.pdf