Safer and Stronger Communities Board
14 January 2012

Item 7

Communications Data Bill

Purpose of report

For information.

Summary

1. The Home Office has informed us that they have not accepted our business case for retaining council and Fire and Rescue Authority access to existing forms of communications data. Councils account for only 0.4% of usage of these powers (2 130 requests) but the pre-legislative Committee was extremely critical of councils' errors in the use of the powers which no doubt has played a part in this conclusion. Trading standards, illegal money lending teams and environmental health officers believe that loss of these powers will significantly constrain councils' powers of investigation into rogue traders, benefits cheats and environmental crime.

2. The Home Office have asked us to resubmit a business case outlining:

    2.1 The impact of losing these powers;
    2.2 Whether it is possible for other public bodies to access data on behalf of councils; and
    2.3 any EU requirements for council to access this data

3. The Joint Committee scrutinising the Communications Data Bill produced its report in late December. The Committee did not recommend that councils be named on the face of the bill but did commend the work of the council-led National Anti-Fraud Network and outlined several ways in which safeguards could be put in place to ensure councils access the data in a responsible and proportionate fashion.

4. The LGA has the support of BIS, Trading Standards Institute and the National Anti-Fraud Network and is coordinating responses with them. The Association of Chief Trading Standards Officers (ACTSO) are producing a template letter for councils to send to their local MP outlining the severe impact that would result from loss of access to this data.

5. The following Appendices are included:

    5.1 **Appendix A**– Draft response to the Home Office
    5.2 **Appendix B** – Copy of the Home Office letter to the LGA
    5.3 **Appendix C** – Summary of the Joint Committee report into the Bill

Recommendation

That Members note the report.

Action

LGA officers to progress as appropriate.

Contact officer: Gwyneth Rogers / Ian Leete
Position: Senior Adviser – regulation, Adviser - regulation
Phone no: 020 7664 3861 / 3143
E-mail: gwyneth.rogers@local.gov.uk / ian.leete@local.gov.uk

Local Government Association

Safer and Stronger Communities Board

14 January 2012

Item 7

Communications Data Bill

Background

1. The Draft Communications Data Bill outlines government proposals for safeguards around the use of communications data by public bodies. The Bill would replace the framework included within the Regulatory Investigatory Powers Act (RIPA) for communications data only.

2. The Bill proposes to increase the data accessible to law enforcement, national security agencies and other public bodies in order keep pace with technological change. It is not proposed that councils have access to this expanded data set.

3. The Draft Bill was published with only the police, intelligence agencies and HMRC named on the face of the Bill. The Home Office requested that all other public bodies submit a business case to justify continued access to communications data. These powers would only be provided under secondary legislation and there is currently no indication of the government position about whether councils should retain access to communications data under this approach.

4. The LGA has submitted a business case on behalf of councils and FRAs. Although Home Office officials tell us our evidence was considered to be stronger than a number of public agencies, it was not considered to be sufficient to include councils on the face of the bill. This is due in part to the lack of an evidence base demonstrating the outcomes resulting from access to communications data; councils record successful prosecutions by the type of crime committed and are unable to easily identify which cases may have used communications data. There is also a political imperative to significantly reduce the number of public bodies accessing the data; councils are considered individually rather than collectively in this and therefore make up a very significant proportion of the list of public bodies with access.

5. Government is now considering the Joint Committee's report and will be drafting amendments with a view to introducing the Bill in the next session. It is expected that the Bill will subject to considerable debate following opposition by the Liberal Democrats.

Paul Regan
Deputy Director

Home Office - OSCT
Pursue Policy and Strategy Unit
5th Floor Peel Building
2 Marsham Street
London
SW1P 4DF

10 January 2013

Dear Paul

COMMUNICATIONS DATA POWERS

Thank you for your letter of 21 December advising that Government has, at this stage, rejected the need for councils and Fire and Rescue Authorities (FRAs) to access communications data. It is helpful that you have recognised that there is further information to be considered before a final decision is made and I am now attaching information in response to your request. We have also asked local authorities to respond directly to you providing individual responses about their local area which I hope will provide further evidence.

We share many of the concerns of the Coalition government about ensuring that access to this data respects the right of the individual to privacy, while at the same time providing enforcement agencies with the tools to protect people from exploitation. Councils are responsible enforcement agencies with a genuine need to access some elements of this data and we wish to work with the Government to ensure that these tools are fit and proportionate for use in the modern context.

Although we were disappointed that the Joint Committee did not explicitly recommend that councils were named on the face of the Bill, there are many instances where the committee outlines ways in which appropriate safeguards could be put in place for councils to access the data in future. For instance, they specifically commended the council-led National Anti-Fraud Network as an example of expertise and recommended that 'all local authorities and other infrequent users of communications data should be required to obtain advice from this service' or a service modelled on it.

We worked closely with Government on the Protection of Freedoms Act to introduce a new threshold of six months imprisonment below which an application to conduct surveillance could not be made. Preliminary reports from NAFN and council officers suggest that this is working well and we believe it provides a current and effective model for ensuring that communications data is used for only serious offences as is intended by Home Office ministers. It would therefore be good to have a conversation about what additional safeguards Ministers might want to see in place for communications data powers, such as application of a similar threshold, which would allow councils to be included in the list of agencies retaining the powers.

I know that the Government wants to see the continued protection of consumers continue and there is a real risk that the ability to take swift and effective action will be undermined without access to these powers.

As requested, I have addressed your three key questions below, but must emphasise that council use of these powers is driven by a need to protect residents and responsible businesses. If you have any further queries about councils' need to retain their existing powers of access to communications data then please do not hesitate to contact me.

Yours sincerely

Helen Murray
Programme Director, Safer and Stronger Communities

CC: Neil O'Connor, Director, FRED, DCLG

1. Impact

Councils use communications data to protect residents and businesses from those that are deliberately and purposefully trying to cause harm. Losing access to communications data would leave councils and fire authorities without the tools to protect residents and allow criminals to operate more freely in our communities. Although these powers are used infrequently, they are a valuable part of councils' toolbox to tackle crime.

We are not requesting additional, expanded access to the new communications data content, but we are keen that local authorities are able to continue to use their existing powers which are essential to the work carried out by councils. There are a number of crucial offences for which councils are the main enforcement body, including benefits and council tax fraud, metal theft, rogue traders, loan sharks, doorstep crime, serious environmental crime, commercial flytippers, and counterfeit goods. At no point will councils require access to the content of the communications or any of the information contained in Clause 1 of the Bill and we do not ask for this access.

The new draft Bill retains several permitted reasons for accessing data that are the responsibility of councils, but not part of the core function of the police or other public bodies:

- (d) in the interests of the economic well-being of the United Kingdom,
- (e) in the interests of public safety,
- (f) for the purpose of protecting public health,

The investigation of some particularly heinous crimes is enhanced by councils having access to these powers. In particular, the prosecution of a number of environmental crimes, including metal theft rests on being able to link individuals to the sale of stolen goods through mobile phone usage and councils would not want to see that ability reduced.

High profile consumer protection initiatives such as Scambusters, Loan Sharks and the increasingly topical issue of illegal money lending are also likely to be significantly affected.

Phone records may provide valuable evidence to bring criminals to justice. For example, in a current case, a trader charged around £100,000 for work which wasn't done or wasn't necessary. In interview it has been claimed that work was only done at the victim's request and that he rang one of the offenders on each occasion to request work. The victim's outgoing call logs have been requested to disprove that. It illustrates an important part of the offenders' conduct and in particular, the fact that one offender was prepared to lie in interview.

Council Trading Standards officers also enforce much of the consumer protection legislation, which can save consumers up to £40 million a year. In 2010, council officers tackling illegal moneylending helped 11, 500 people write off more than £31 million of illegal debt and pursued a further £10 million of criminal assets through the courts. Access to communications data forms a numerically small part of this work, but can provide the critical evidence to secure a conviction for larger crimes sometimes involving sums of £400 000. A loss of access to this data could see offenders failing to be tracked down and prosecuted at all as they cannot be connected to the crime.

2. Shared agreements

It is probable that a shared agreement with the police could work well for FRAs, as their use of communications data usually relates to core police activities such as the investigation and prosecution of arson. However, councils access data for a number of reasons that do not correlate well the core priorities of the police.

Councils work closely with the police to prevent crime and we agree that further joint-working can be developed to maximise the efficient use of resources. It is important to recognise, however, that police forces are also under pressure and we would question whether they have the existing capacity or expertise to tackle complex issues such as benefit fraud.

Although local authorities would be able to negotiate shared agreements, data sharing still presents barriers at the local level if councils are not named in the Bill. It would be more proportionate and effective to look at alternative safeguards through either the magistrates system used by the Protection of Freedoms Act, or strengthening the role of the SPoC as recommended by the Joint Committee. A strengthened SPoC role could mean the Home Office accrediting expert organisations to provide this function, which could open up the market to competition.

We agree with the principle expressed by the Joint Committee that the public need reassurance that decisions to request data are evaluated with an appropriate understanding and expertise in the law. However, establishing a centralised service with no flexibility about alternative models that could deliver the same outcomes would remove the process from the local context and political accountability that we believe is crucial to reassuring the public.

NAFN has proven an effective resource for many councils and they have an excellent track record of ensuring data requests are of a high quality, but there is a cost to access their service and this is considered prohibitive for some councils. Rather than establish a new organisation in legislation, as suggested by the committee, we believe that providing formal resource from the Home Office to make NAFN's services affordable for all councils would deliver the needed reassurance of expertise in a timely and cost effective fashion, and without requiring the establishment of a new quango.

3. European responsibilities

EU law, or the subsequent UK regulations frequently refer to council officers as a responsible enforcement body and removing their access to data risks the possibility of infraction proceedings, which would be costly to contest even if successfully challenged.

The Unfair Commercial Practices Directive, for instance, requires administrative authorities to be able to secure evidence against a trader responsible for 'making persistent and unwanted solicitations by telephone, fax, e-mail or other remote media'. The UK has implemented this directive through the Consumer Protection from Unfair Trading Regulations 2008, which sets out evidential requirements in clause 27. It will be extremely difficult to enforce this requirement without access to communications data.

This view is shared by the 40 consumer organisations in EU member states who responded to the Commission's questionnaire on the application of the Directive by saying "In the absence of written documents, it is very difficult for the consumer to proof [sic] these aggressive practices."

Safer and Stronger Communities Board
14 January 2012

Item 7

Appendix B

Dear Colleague

COMMUNICATIONS DATA POWERS

As you know, the Home Office is planning to legislate to replace the provisions in Part 1 Chapter 2 of the Regulation of Investigatory Powers Act 2000 (RIPA), which currently provides for Local Authorities to acquire communications data.

I wrote on 11 December following the publication of the report of the Joint Committee on the Draft Communications Data Bill. One of the issues that the Committee considered was which public authorities should have access to communications data. The Committee concluded that it expected the list of public authorities with such access to be "greatly reduced" when compared to the existing position.

Ministers are committed to giving effect to the substance of all of the Joint Committee's recommendation. Their starting point, in respect of which public authorities should have access, is that only those for whom the strongest case can be made should retain their powers.

Ministers have considered the business cases submitted to the Home Office earlier in the year outlining your rationale for access to communications data, and your need for the powers in future, but consider that, in the light of the Joint Committee's report, your organisation has not made a compelling case for inclusion.

We therefore need to establish what the effect would be for Local Authorities if you did not retain access to communications data under the proposed legislation. As well as this, Ministers wish to consider whether your organisation would require the new data that would be available under clause 1 of the proposed Bill – that is generated data not presently retained for business purposes, including that from overseas providers.

To this end, it would be useful if you could provide clear answers to the following three questions.

1. What would be the impact if you cannot access communications data at all?
2. If you lose the ability to acquire communications data in your own right, would it be possible for you to form agreements with another public authority to acquire communications data on your behalf, where it is necessary and proportionate to do so?
3. Are there any requirements in EU law that you must be able to access communications data? If so, where? If you lose this ability, what would be the likely impact?

I would be grateful for reply by 16 January. It is crucial that we receive this information in this timeframe, so that Ministers can make an informed consideration before making a final decision on which bodies will retain their powers.

If you would like to discuss this request further, please contact the Communications Data team on 0207 035 6816 draftcommsdatabill@homeoffice.x.gsi.gov.uk.

Local Government Association

Safer and Stronger Communities Board

14 January 2012

Item 7

Appendix C

Key findings of the Joint Committee on the Draft Communications Data Bill affecting councils

Key finding - The Home Office should not have assumed a consultation paper published in April 2009 could justify the publication of draft legislation three years later without further consultation with the public and those most closely affected by it proposals.

LGA position – The consultation exercise has not proved meaningful or constructive and as such has been flawed. The launch of the draft Bill signalled the start of a process that has proved confusing for councils and wider stakeholders. The request for a Business Case from the Home Office to retain powers contradicted both a clause in the draft Bill about how councils could use their powers and a parallel request for evidence from the Bill Committee. The Bill Committee seemed unaware that the Home Office request for business cases had even been made.

The Home Office failed to consult with Fire and Rescue Authorities until a very late stage, leaving little time for constructive input.

The Government position on which public bodies will retain communications data powers remains wholly unclear, and urgent clarity is needed.

Key finding - In 2011 141 local authorities notified the Interception of Communications Commissioner that they had made a total of 2130 requests, which is just 0.4% of all communications data requests submitted by public authorities. Despite this, local authorities accounted for 9% of the reportable errors. This is 20 times the average of other public bodies. The evidence we have received shows that errors by local authorities cause public concern out of all proportion to the numbers involved. This seems to be because examples of misuse or abuse of the system are not only relatively frequent, but also particularly alarming.

The IoCC reports that, of the 141 local authorities which notified him that they had made use of their powers in 2011, 58% had made fewer than 10 requests. This plainly contributes to the number and gravity of the errors: those processing the applications for access to communications data do so infrequently and have relatively little experience of the system.

LGA position – We wholly support the need to reassure the public that this power is only being used as a last resort by councils and with full safeguards and scrutiny in place. We recognise that it can be difficult for councils that use such powers so sparingly to maintain levels of expertise, however, many councils are already maximising opportunities such as National Anti-Fraud Network (NAFN) in order to maintain the appropriate levels of knowledge to prevent mistakes occurring. The LGA is keen that councils can learn lessons from mistakes that have been made and would welcome working with the Information of Communications Commission to identify common themes and possible solutions.

Key finding – If it is thought that local authorities, or some of them, should have access to communications data, they should follow the procedure we have suggested for all other public bodies and not have to secure approval from a magistrate.

LGA position – We agree that there should be consistency among public bodies, to both build a common understanding in the public and media about how powers are used and to provide reassurance of the high standards that all public bodies are expected to meet. From 1 November 2012, councils are required to seek the approval of a magistrate for access to communications data. We agree with the Committee that this does not, in itself, provide an additional safeguard.

However, since that policy has now been implemented, we would advocate a period of settling in and a review of the current arrangements to fully explore any added value or problems before abandoning this policy in favour of a different policy.

Key finding - Any public bodies which make a convincing business case for having access to communications data should be listed on the face of the Bill.

LGA position – The LGA submission to the Committee made this suggestion and we are pleased that this is now the recommended approach. The LGA believes that local authorities and fire and rescue authorities should be added to the face of the Bill.

Key finding - The SPoC process should be enshrined in primary legislation. A specialist centralist SPoC service should be established modelled on the National Anti-Fraud Network Service that currently offers SPoC expertise to local authorities. The Home Office should consider allowing police forces to run this service. The new service should be established by statute, and all local authorities and other infrequent users of communications data should be required to obtain advice from this service.

LGA position – We agree with the principle that the public need reassurance that decisions to request data are evaluated with an appropriate understanding and expertise in the law. However, establishing a centralised service with no flexibility about alternative models that could deliver the same outcomes would remove the process from the local context and political accountability that we believe is crucial to reassuring the public.

It is not clear why the committee would recommend that a replacement is found for NAFN when they acknowledge that it is providing excellent service.

Key finding - In the case of local authorities it should be possible for the magistrates to cope with the volume of work involved in approving applications for authorisation. But we believe that if our recommendations are accepted and incorporated into the Bill, they will provide a stronger test than a magistrate can and it will be unnecessary to continue with differing arrangements applying to local authorities.

LGA position – The LGA believes that local scrutiny arrangements, backed up by the Interception of Communications Commissioner for RIPA powers provides the transparency and proportionality sought by the public. This report calls for the requirement for councils to secure sign-off from a magistrate for access to communications data to be scrapped in favour of nationally set authorisation procedures. It is an anomaly for councils to be subject to stricter arrangements than other public agencies and therefore we support the Committee's findings.

Key finding - While sampling is acceptable as a way of dealing with large users, the requests of users making fewer than 100 applications in a year should be checked individually. The annual report of the IoCC should include more detail, including statistics, about the performance of each public authority and the criteria against which judgements are made about performance.

LGA position – Local authorities only seek to use these powers to protect residents and taxpayers from acts of dishonesty, but we recognise that more need to be done to increase transparency about why surveillance powers are sometimes necessary and what they are used for.

The LGA remains committed to increasing the transparency about council use of RIPA powers and we encourage councils to publish their use of these powers in an easily accessible manner

for residents. Increased transparency will provide reassurance to residents that their councils are acting responsibly to protect them.

More detail in the IoCC report would enable local government to address any discrepancies or emerging themes which require attention in terms of the operation of the policy or process.

Key finding - We agree with the Home Office that there is no need for criminal offences to punish minor administrative errors made by officials in public authorities while seeking to acquire communications data. Where appropriate, disciplinary action should suffice. However, the draft Bill should provide for the wilful or reckless misuse of communications data to be a specific offence punishable in appropriate cases by imprisonment.

LGA position – We agree that any response to an error should be proportionate, making use of existing disciplinary powers as employers. We would recommend that the Home Office or Interception of Communications Commissioner record the types of administrative errors discovered, with a view to identifying common mistakes and targeting support to resolving them.

Where there is wilful or reckless misuse of these powers then it is appropriate for there to be a more serious punishment available.